Selected topics on quantum and post-quantum correlations

Paweł Horodecki
Faculty of Applied Physics and Mathematics
Gdańsk University of Technology
National Quantum Information Center of Gdańsk
University of Gdańsk

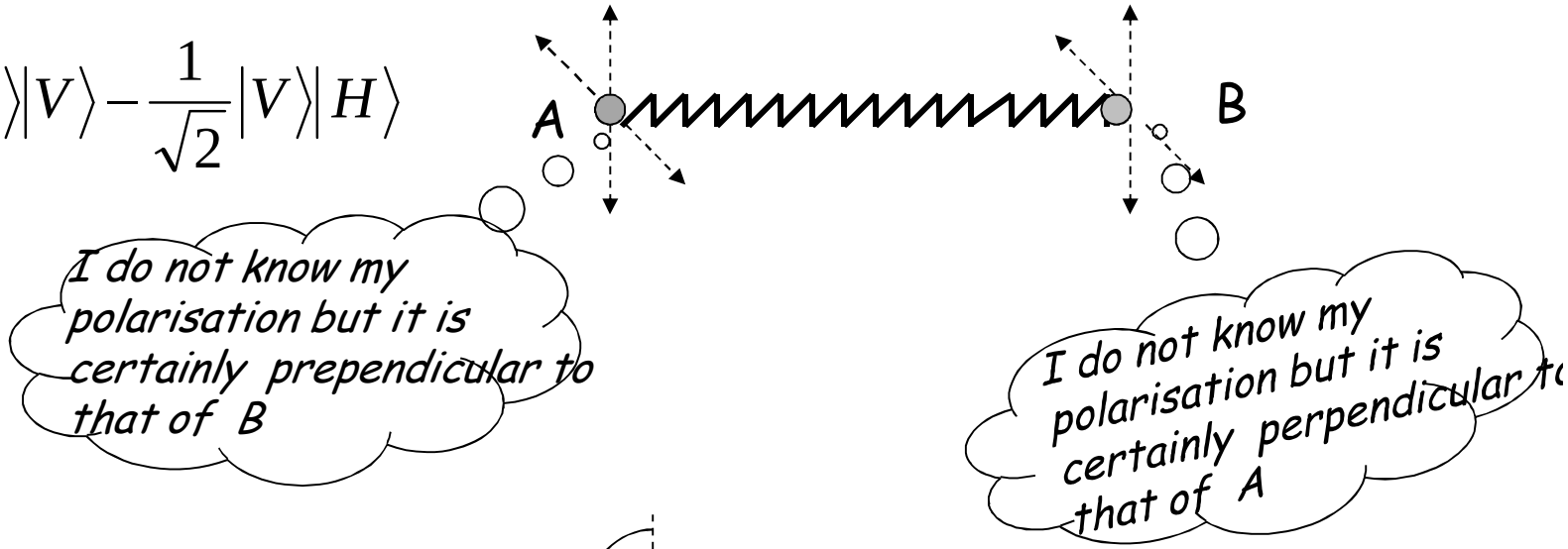
Collaboration within ERC ARG QOLAPS project lead by Ryszard Horodecki
Polish Ministry of Science and Higher Education IDEAS PLUS
John Templeton Foundation project

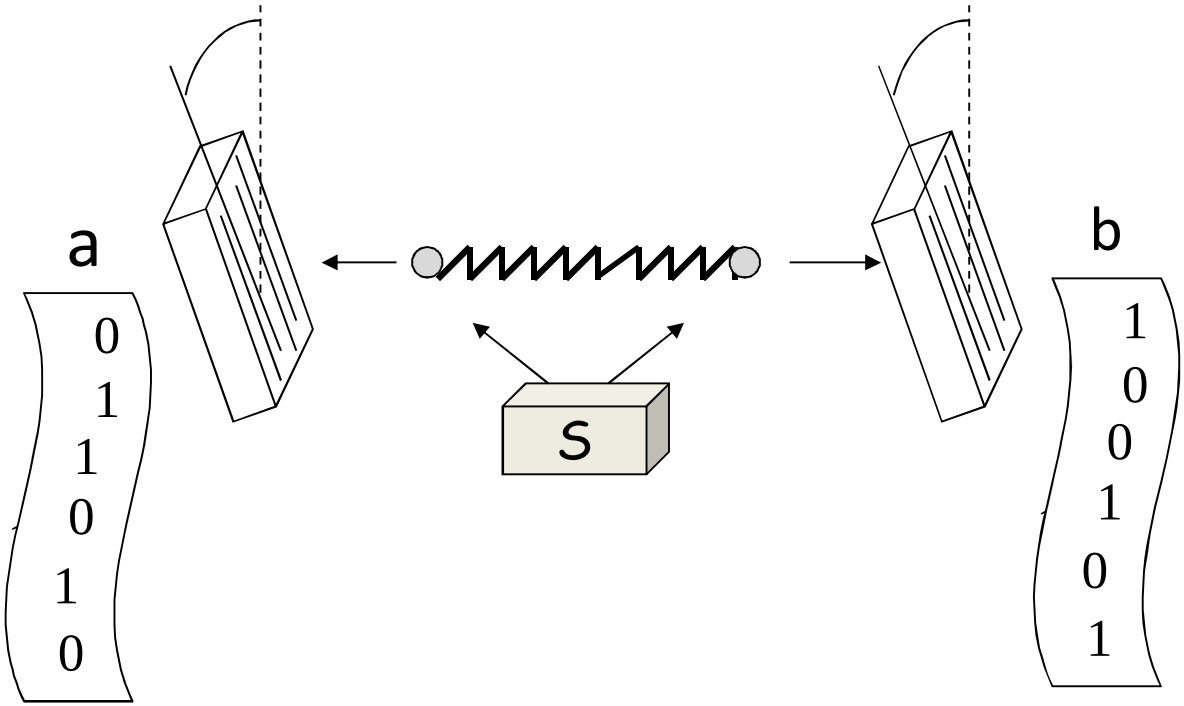
Plan

- Quantum entanglement - introduction
- Classical (LHV), quantum and no-signaling correlations
- Quantum correlations and the issue of faster than light communication
- Describing Q by SDP hierarchy
- Geometry of Q versus NS
- Monogamy of NS correlations
- Communication complexity - a simple example
- Some physical principles aiming at restoring Q
- Violation of Bell inequality and uncertanity relations
- Deriving Bell inequality problem form quantum communication complexity advantage.

Quantum entanglement

$$|\psi\rangle = \frac{1}{\sqrt{2}}|H\rangle|V\rangle - \frac{1}{\sqrt{2}}|V\rangle|H\rangle$$

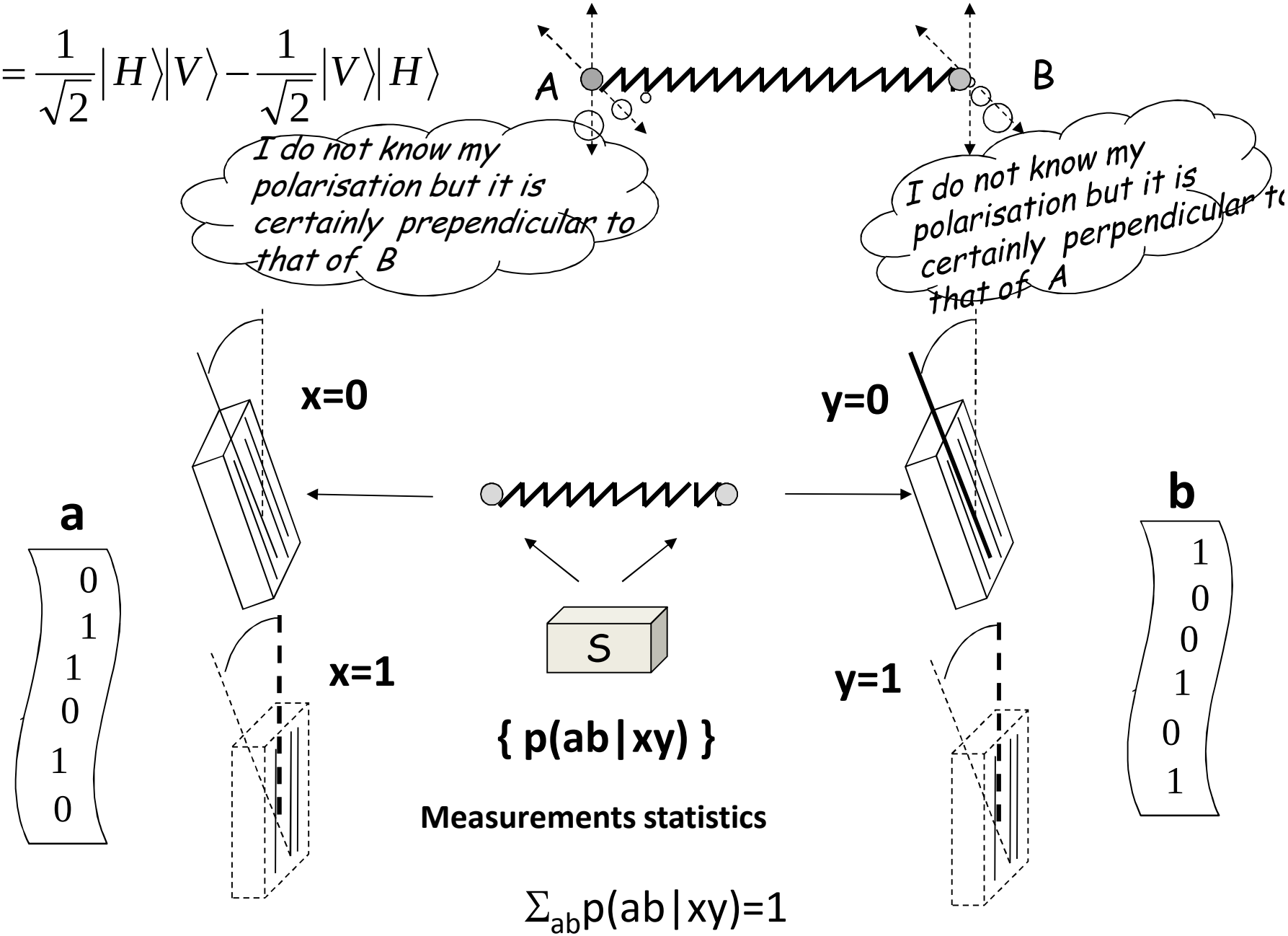




Independently to the distance they,,remember' each other: results always different…

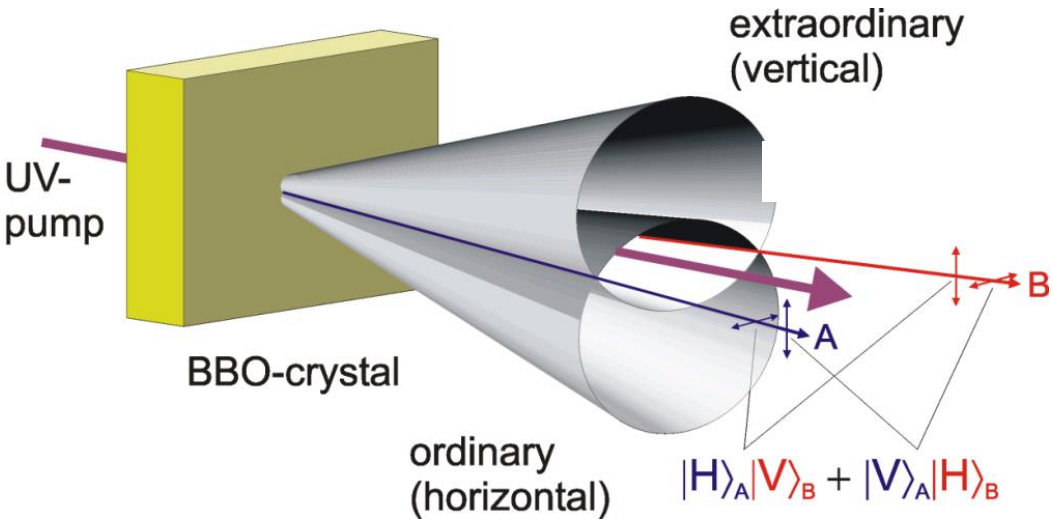
Polarisers – settings

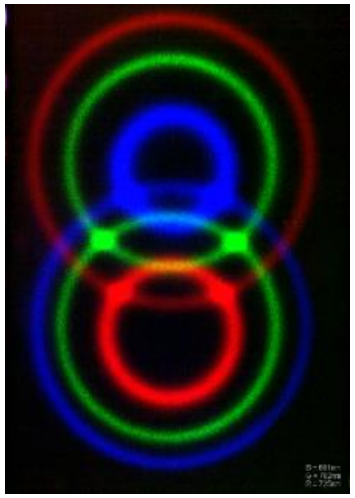
$$|\psi\rangle = \frac{1}{\sqrt{2}}|H\rangle|V\rangle - \frac{1}{\sqrt{2}}|V\rangle|H\rangle$$



$\Sigma_{ab} p(ab|xy)=1$

Preparing entanglement in polarisation





Essence of entanglement of pure state

$$|\Psi_{AB}\rangle \neq |\phi_A\rangle\, |\varphi_B\rangle$$

What are quantum correlations ?

Strong sense - quantum entanglement

(nonentangled state otherwise)

$$\rho_{AB} \neq \Sigma\, \mathbf{p_i}\, |\varphi_i\rangle\langle\varphi_i| \otimes |\psi_i\rangle\langle\psi_i|$$

Weak sense - quantum entanglement **+ some (!) nonentangled states**

In any decomposition some pair locally not orthogonal

$$\rho_{AB} = \Sigma_i\, \mathbf{p_i}\, |\varphi_i\rangle\langle\varphi_i| \otimes |\psi_i\rangle\langle\psi_i|$$

Classical correlations:

Orthogonal

$$\rho_{AB} := \Sigma_{ij}\, \mathbf{p}_{ij}\, |i\rangle\langle i| \otimes |j\rangle\langle j|$$

[H. Ollivier, W. H. Zurek, Phys. Rev. Lett. (2001)]
Alternative approach:
[L. Henderson & J. Vedral, J. Phys. A (2001)],
Thermodynamical approach:
[J. Oppenheim, M. P. &R. Horodeccy , Phys. Rev. Lett. (2002)]

Review on quantum entanglement

REVIEWS OF MODERN PHYSICS, VOLUME 81, APRIL–JUNE 2009

Quantum entanglement

Ryszard Horodecki

Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland

Paweł Horodecki

Faculty of Applied Physics and Mathematics, Technical University of Gdańsk, 80-952 Gdańsk, Poland

Michał Horodecki

Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland

Karol Horodecki

Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland
and Faculty of Mathematics, Physics and Computer Science, University of Gdańsk, 80-952 Gdańsk, Poland

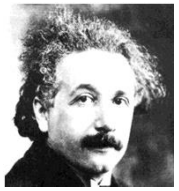
(Published 17 June 2009)

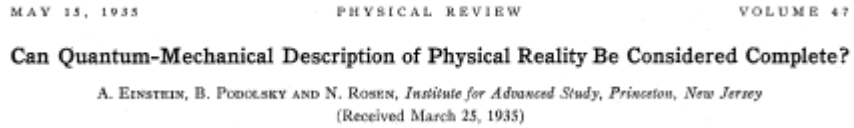
All our former experience with application of quantum theory seems to say that *what is predicted by quantum formalism must occur in the laboratory*. But the essence of quantum formalism—entanglement, recognized by Einstein, Podolsky, Rosen, and Schrödinger—waited over 70 years to enter laboratories as a new resource as real as energy. This holistic property of compound quantum systems, which involves nonclassical correlations between subsystems, has potential for many quantum processes, including canonical ones: quantum cryptography, quantum teleportation, and dense coding. However, it appears that this new resource is complex and difficult to detect. Although it is usually fragile to the environment, it is robust against conceptual and mathematical tools, the task of which is to decipher its rich structure. This article reviews basic aspects of entanglement including its characterization, detection, distillation, and quantification. In particular, various manifestations of entanglement via Bell inequalities, entropic inequalities, entanglement witnesses, and quantum cryptography are discussed, and some interrelations are pointed out. The basic role of entanglement in quantum communication within a distant laboratory paradigm is stressed, and some peculiarities such as the irreversibility of entanglement manipulations are also discussed including its extremal form—the bound entanglement phenomenon. The basic role of entanglement witnesses in detection of entanglement is emphasized.

DOI: 10.1103/RevModPhys.81.865 PACS number(s): 03.67.−a

The debate on entanglement and determinism

Quantum mechanics: polarisations NOT DEFINED before measurement





MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

A. Einstein: QM is incomplete.
True polarisations are determined (EPR elements of reality)

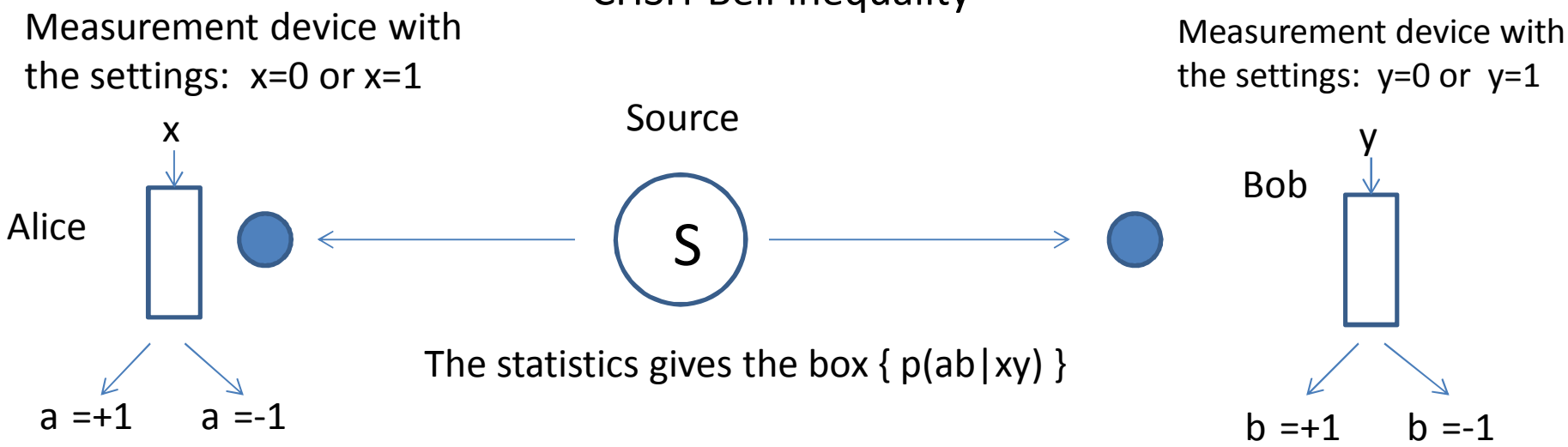
N. Bohr: indeterminism in QM has a fundamental character - problem with notion of reality*

John Bell (1928-1990): QM ,,is right", The polarisation is undefined (to imagine that it is not, leads to the conclusions in contradiction with experiment -> Bell inequalities).

Alain Aspect Experiment, 1981

Conclusion: distant particles at the some time acquire the properties NOT PRESENT BEFORE !

CHSH-Bell inequality



The statistics gives the box { p(ab|xy) }

Mean value $\langle A_x B_y \rangle = \Sigma_{ab=\pm 1}\, ab\, p(ab|xy)$ (correlation quantity)

Mean value of Bell operator $\langle B \rangle = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle$

Bell inequality (LHV): $\langle B \rangle \leq 2 = C_{LHV}$

Quantum (Tsirelson) bound: $\langle B \rangle \leq 2\sqrt{2} = C_Q$

No-signaling bound: $\langle B \rangle \leq 4 = C_{NS}$

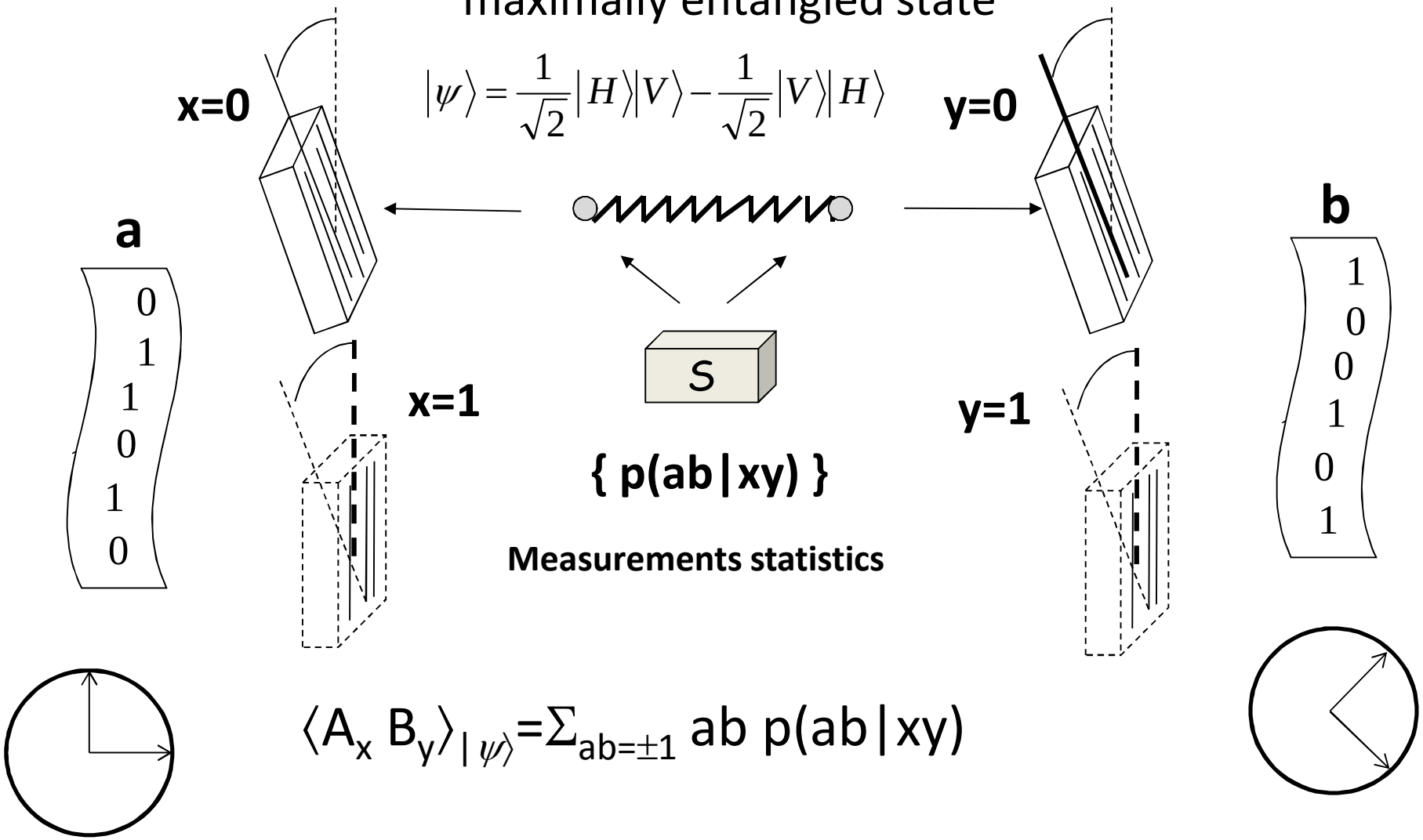
$C_{LHV} < C_Q < C_{NS}$

(all the bounds are saturated within the corresponding classes of boxes)

Bell inequality violation by quantum mechanics

Saturation of quantum bound by measurements on maximally entangled state

$$|\psi\rangle = \frac{1}{\sqrt{2}}|H\rangle|V\rangle - \frac{1}{\sqrt{2}}|V\rangle|H\rangle$$

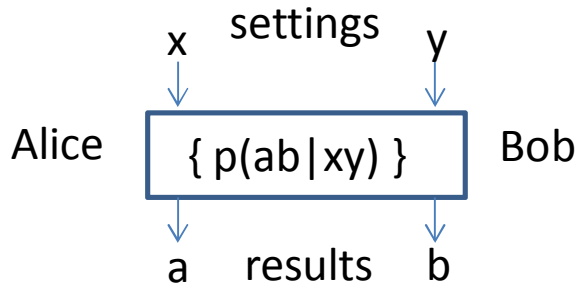


$$\langle A_x B_y \rangle_{|\psi\rangle} = \Sigma_{ab=\pm 1}\, ab\, p(ab|xy)$$

$$\langle B \rangle_{|\psi\rangle} = \langle A_0 B_0 \rangle_{|\psi\rangle} + \langle A_0 B_1 \rangle_{|\psi\rangle} + \langle A_1 B_0 \rangle_{|\psi\rangle} - \langle A_1 B_1 \rangle_{|\psi\rangle} = \mathbf{2\sqrt{2}}$$

Theory of no-signaling boxes – important subclasses

No-signaling (NS) boxes : [S. Popescu & D. Rohlich 1994]



$\{ p(ab|xy) \}_{a,b,x,y}$ family of conditional probabilities

$$\left.\begin{aligned} \Sigma_b p(ab|xy) &:= p(a|xy) = p(a|x) \\ \Sigma_a p(ab|xy) &:= p(b|xy) = p(b|y) \end{aligned}\right\} \text{ No-signaling conditions}$$

Quantum (Q) boxes:

$$p(ab|xy) = \mathrm{Tr}(M_{a|x} \otimes M_{b|y}\, \rho_{AB})$$

$$\Sigma_a M_{a|x} = I_A, \quad 0 \le M_{a|x} \le I_A$$
$$\Sigma_b M_{b|y} = I_B, \quad 0 \le M_{b|y} \le I_B$$

Usually local quantum observables:

$$A_x = \Sigma_a \lambda_{a,x}\, E_{a|x}, \; B_y = \Sigma_a \lambda_{b,y}\, F_{b|y}$$

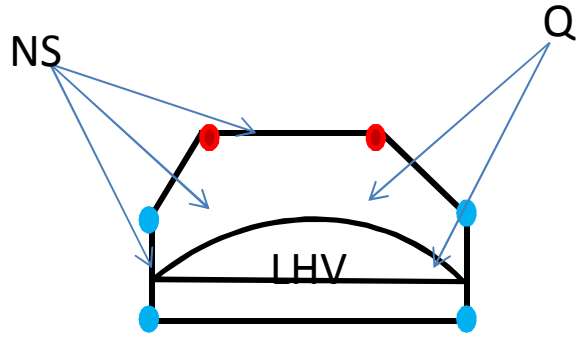
with orthogonal projectors $E_{a|x} E_{a'|x} = \delta_{x x'} E_{a|x}$

$$F_{a|x} F_{a'|x} = \delta_{x x'} F_{a|x}$$

Local hidden variable (LHV) boxes:

$p(ab|xy) = \Sigma_\omega p(\omega)\, p_\omega(a|x)\, p_\omega(b|y)$, ω - hidden variable

LOCAL ELEMENTS OF REALITY



If the state ρ_{AB} is separable ⇒ Q = LHV.
If the state ρ_{AB} is entangled the sets usually are not equal to each other

LHV ⊂ Q ⊂ NS

Bell inequalities and games

Bell value (rewritten) $\mathcal{B} = \Sigma_{abxy}\ p(x,y)\ V(a,b|x,y)\ p(a,b|x,y)$

Measurement settings probabilites

Function testing nonlocality

Probabilities of results

Bell inequality

$$\mathcal{B} \leq C_{LHV} \leq C_{QM} \leq C_{NS}$$

Indicator function

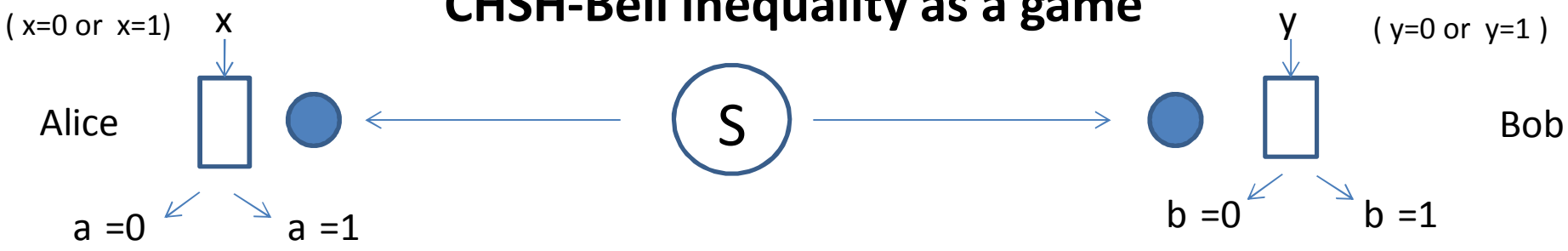
Bell game-type value: $\mathcal{B}_{game} = \mathcal{P}_{win} = \Sigma_{abxy}\, p(x,y)\ \chi(a,b|x,y)\ \ p(a,b|x,y)$

$\mathcal{P}_{win}$ probability of winning the game.
Goal of the game: getting specific outcomes (a,b) for inputs x, y at the a priori fixed statistics p(x,y).

Bell game-type inequality $\mathcal{B}_{game} \leq C_{LHV} \leq C_{QM} \leq C_{NS} \leq 1$

If the settings independent we have **free games**: p(x,y)=p(x)p(y)

CHSH-Bell inequality as a game



$\{ p(ab|xy) \}$

$$\mathcal{B}_{win} = \Sigma_{abxy}\, p(x,y)\, \chi_{CHSH}(a,b,x,y)\, p(a,b|x,y)$$

Bell game-type inequality

$$\mathcal{B}_{win} \leq \underset{3/4}{C_{LHV}} < \underset{1/2 + 1/(2\sqrt{2}) < 1}{C_{QM}} < C_{NS} = 1$$

$\chi_{CHSH}(a,b,x,y)$

x	a \ b	y=0, b=0	y=0, b=1	y=1, b=0	y=1, b=1
0	0	1		1	
	1		1		1
1	0	1			1
	1		1	1	

x \ y	0	1
0	1/4	1/4
1	1/4	1/4

$\{p(x,y)\}$ - independent random settings

$$\chi(a,b|x,y) = 1 \Leftrightarrow a \oplus b = x.y$$

General definition: **XOR games :** $\chi(a,b|x,y) = 1 \Leftrightarrow a \oplus b = f(x,y)$

(possibly more settings)

CHSH-Bell inequality (II)

NS = no-signaling polytope

{ p(ab|xy) } – table representations:

x	a \ b	y=0, b=0	y=0, b=1	y=1, b=0	y=1, b=1
0	0	1			1
	1				
1	0	1			1
	1				

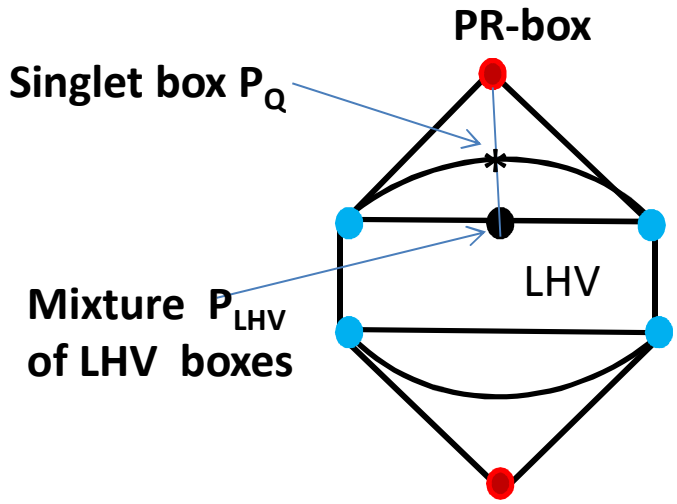
Deterministic NS-extremal point.
Generates all NS-extremal points that are LHV.

x	a \ b	y=0, b=0	y=0, b=1	y=1, b=0	y=1, b=1
0	0	1/2		1/2	
	1		1/2		1/2
1	0	1/2			1/2
	1		1/2	1/2	

Indeterministic NS-extermal points - PR box
Generates all NS-extremal points which are not LHV

x	a \ b	y=0, b=0	y=0, b=1	y=1, b=0	y=1, b=1
0	0	p/2	q/2	p/2	q/2
	1	q/2	p/2	q/2	p/2
1	0	p/2	q/2	q/2	p/2
	1	q/2	p/2	p/2	q/2

$p+q=1$
$p=1/2+\sqrt{2}/4$
$q=1/2-\sqrt{2}/4$

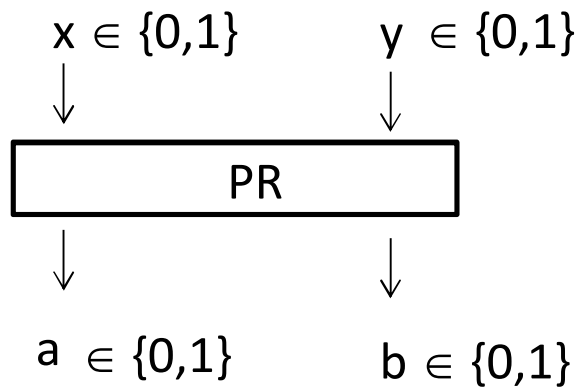


Quantum extremal point – „Singlet box" (generated by the state $|\Psi\rangle=(|0\rangle|0\rangle+|1\rangle|1\rangle)/\sqrt{2}$ (extremal in Q but not in NS !)

PR box as an example of nosignaling correlations (I)

Popescu Rohlich box (1994). Binary inputs (”two settings”), binary outputs.

$$p(ab|xy) = \begin{cases} \frac{1}{2} & (a, b):\ a \oplus b = x\,y \\ 0 & \text{otherwise} \end{cases}$$



Remark. Notice that $a \oplus b = (a+b) \bmod 2$
so $a \oplus b = 0$ unless $x=y=1$ means
,,a = b unless x=y=1 when they are opposite’’.

Normalisation. $\Sigma_{ab} p(ab|xy)=1$ means:
,,sum = 1’’ for any square with fixed x,y.

No – signaling (NS). Why is it no-signaling ?

$\Sigma_b p(ab|xy) := p(a|xy) = p(a|x)$ means: in any **row** sums for the small rectangles are equal (**no y-dependence**)

$\Sigma_a p(ab|xy) := p(b|xy) = p(b|y)$ means: in any **column** sums for the small rectangles are equal (**no x – dependence**)

Table of conditional probablities.

	y	0		1	
x	a \ b	0	1	0	1
0	0	1/2		1/2	
	1		1/2		1/2
1	0	1/2			1/2
	1		1/2	1/2	

PR box as an example of nosignaling correlations (II)

p(ab|xy)

x	a \ b, y	0	1	0	1
0	0	1/2		1/2	
	1		1/2		1/2
1	0	1/2			1/2
	1		1/2	1/2	

$$\Sigma_b\, p(ab|xy) := p(a|xy) \overset{?}{=} p(a|x)$$

x	a \ y	0	1
0	0	1/2	1/2
	1	1/2	1/2
1	0	1/2	1/2
	1	1/2	1/2

p(a|x1)

p(a|x0)

Columns the same **:= p(a|x)**

Signaling box :

q(ab|xy)

x	a \ b, y	0	1	0	1
0	0	1/2		1/3	1/3
	1		1/2		1/3
1	0	1/2			1/2
	1		1/2	1/2	

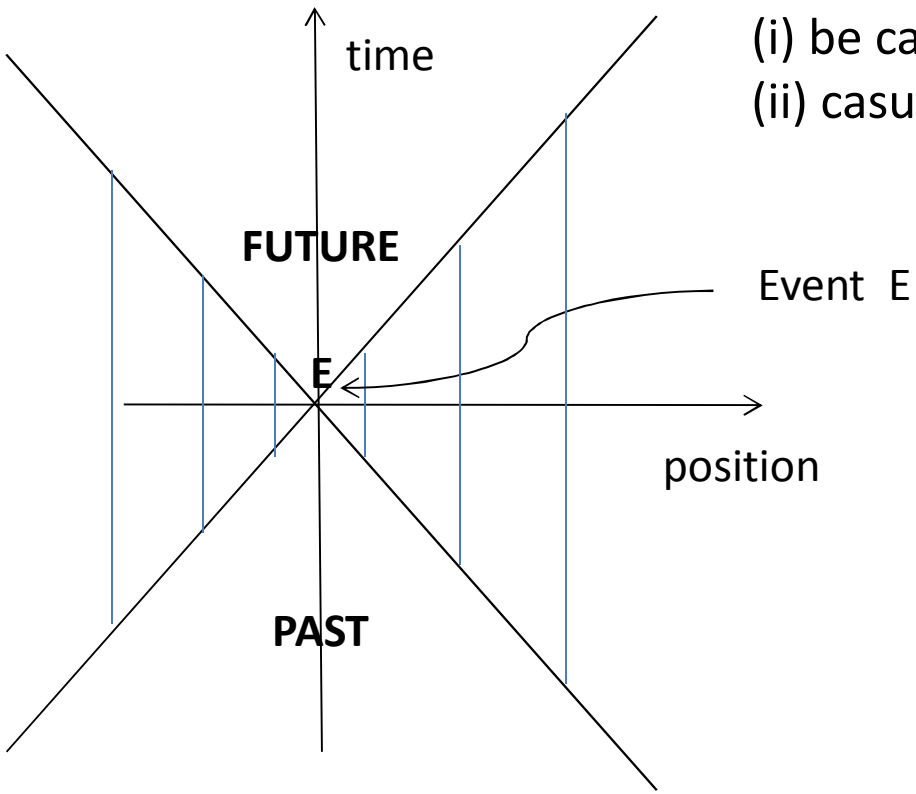
$$\Sigma_B\, q(ab|xy) := q(a|xy) \neq q(a|x)$$

x	a \ y	0	1
0	0	1/2	**2/3**
	1	1/2	**1/3**
1	0	1/2	1/2
	1	1/2	1/2

$$q(a|x0) \neq q(a|x1)$$

Using the box many times Alice can inferr Bob setting y (either 0 or 1) with high probability.

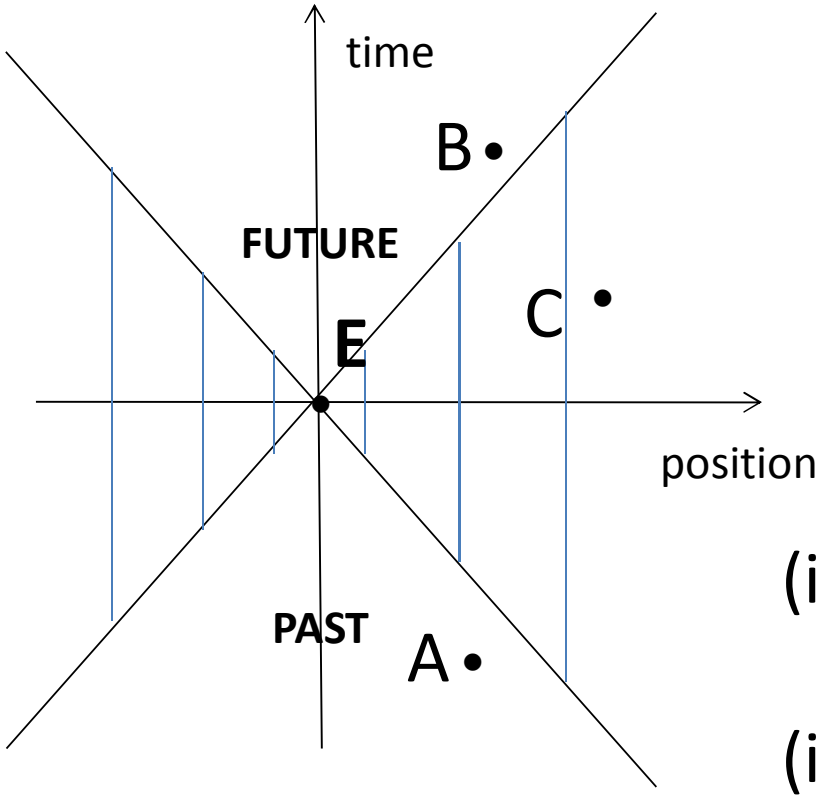
Space-time and the faster than light speed issue



Event E can:
(i) be casually influenced by its PAST
(ii) casually influence its FUTURE

Event E

Space-time and the faster than light speed issue



Event E can:
(i) be casually influenced by its PAST
(ii) casually influence its FUTURE

E can

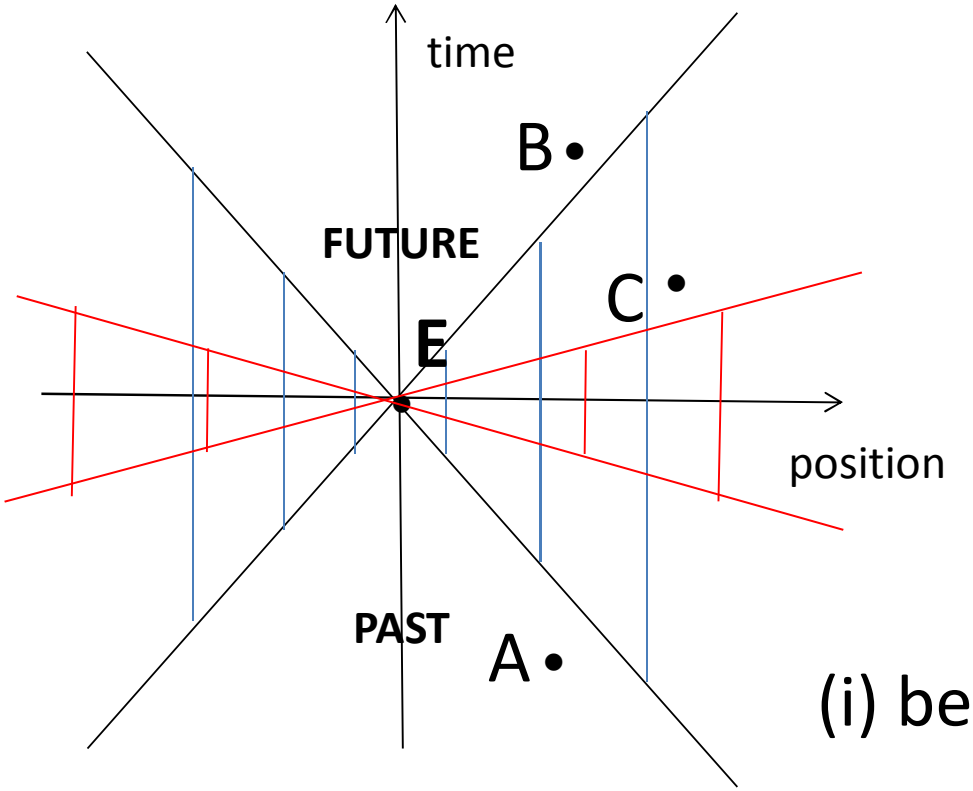
(i) be influenced by A: $E < A$

(ii) influence B: $B < E$

(iii) neither influence
nor be influenced by C: $E \sim C$

What if the speed of light were $v > c_{light}$?

Space-time and the faster than light speed issue



Event E can:
(i) be casually influenced by its PAST
(ii) casually influence its FUTURE

E can

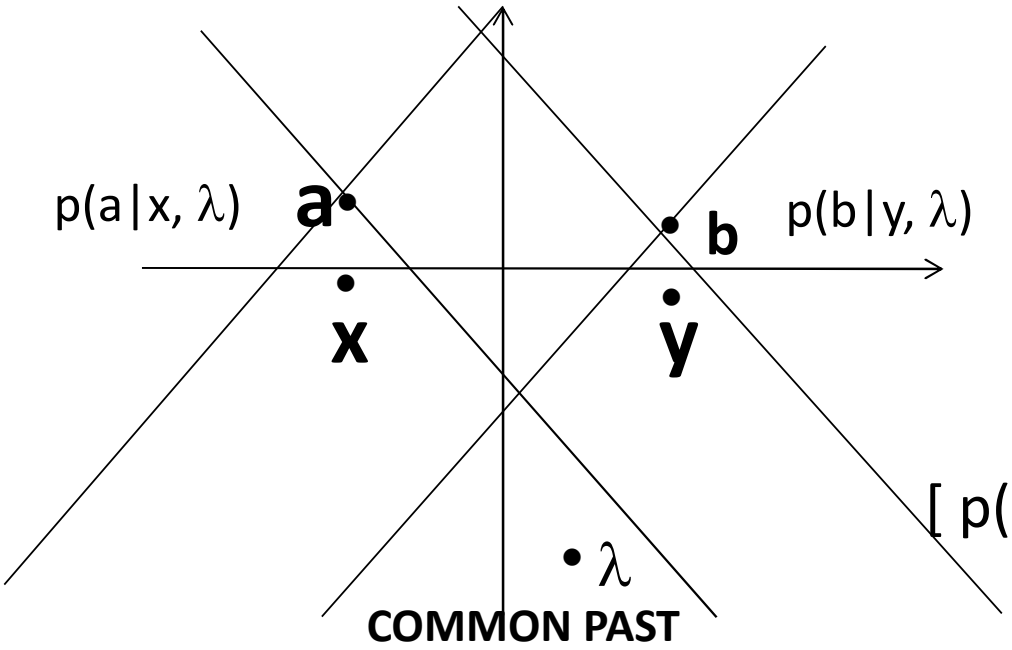
(i) be influenced by A: $E <_v A$

(ii) influence B: $B <_v E$

(iii) influence C: $E <_v C$

$V > C_{light}$

Space-time and the faster than light speed issue



Generally

$$p(a,b,x,y|\lambda) = p(a,x|\lambda)\, p(b,y|\lambda)$$

Settings x, y before a, b so

$$p(a,b,x,y|\lambda) =$$

$$[\, p(a|x,\lambda)\, \underbrace{p(x|\lambda)}_{p(x)} \,]\, [p(b|y,\lambda)\, \underbrace{p(x|\lambda)}_{p(y)} \,]$$

"Free will" assumption

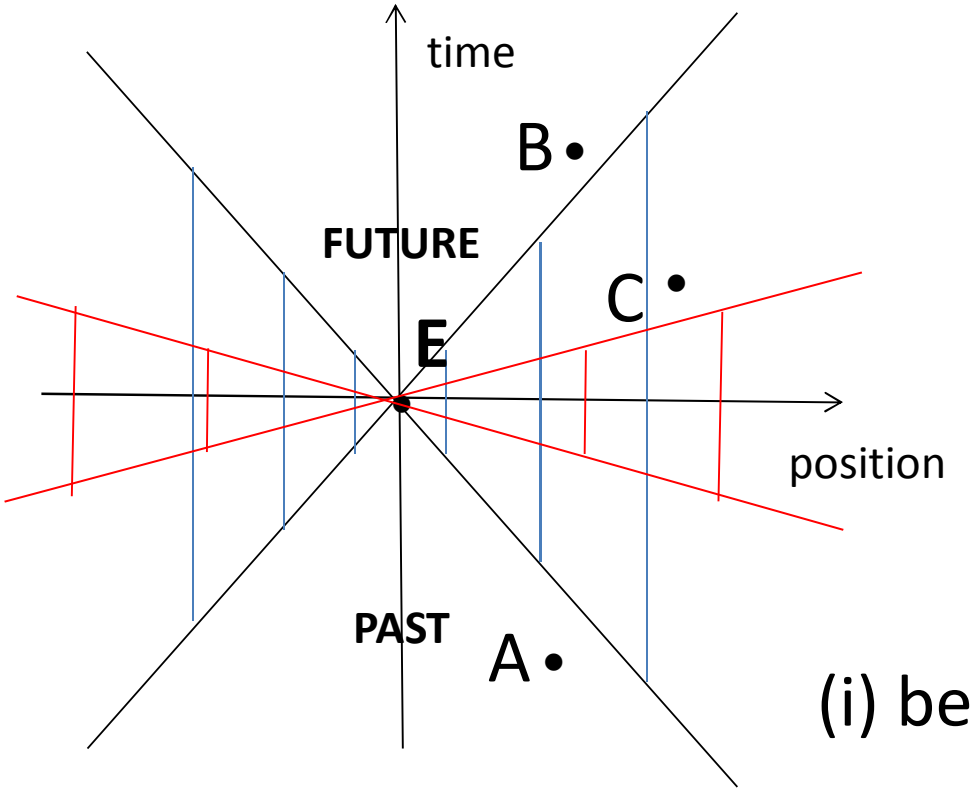
$$p(a,b,x,y|\lambda) = p(a|x,\lambda)\; p(b|y,\lambda)\, p(x)\, p(y)$$ or, after coditioning

$$p(a,b|x,y,\lambda) = p(a,b,x,y|\lambda)/\,[p(x)\, p(y)] = p(a|x,\lambda)\; p(b|y,\lambda)$$

$$p(a,b|x,y) = \Sigma_\lambda\, p(\lambda)\, p(a,b|x,y,\lambda) = \Sigma_\lambda\, p(\lambda)\, p(a|x,\lambda)\; p(b|y,\lambda)$$

(average over λ needed since we do not know its statistics)

Influences of $v > c_{light}$



Event E can:
(i) be casually influenced by its PAST
(ii) casually influence its FUTURE

E can

(i) be influenced by A: $E <_v A$

(ii) influence B: $B <_v E$

(iii) influence C: $E <_v C$

$V > C_{light}$

Can quantum statistics be explained locally via some speed $v > c_{light}$?

Cosinder four-party box $p(abcd|xyzw)$

(i) Assume that its BC are locally explained by some superluminal speed $v > c_{light}$ due to $A <_v D <_v B \sim_v C$.

$$p(bc|yz;axdw) = \Sigma_\lambda\, p(\lambda|axdw)\, p(b|y,\lambda)\; p(c|z,\lambda)$$

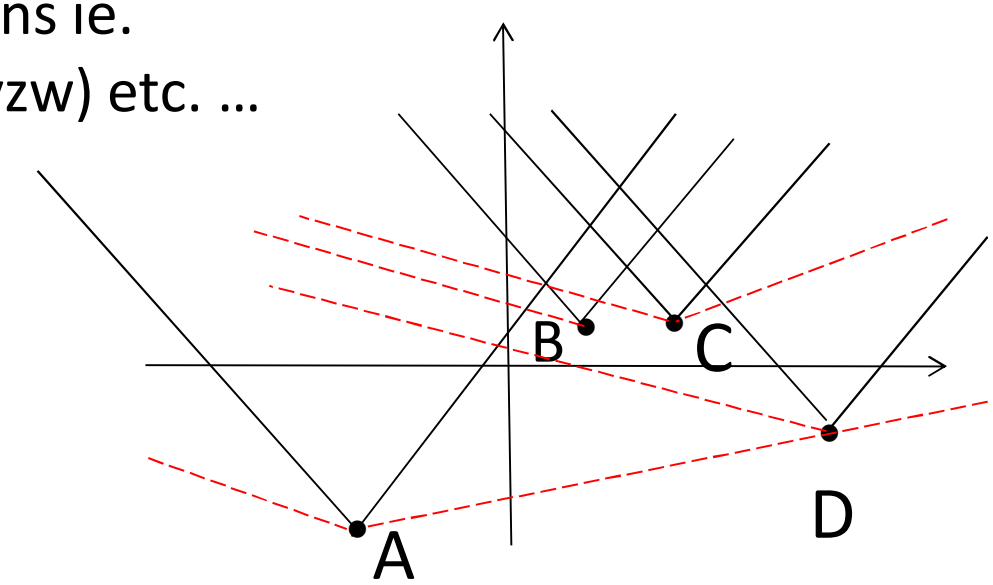
(ii) Assume it satifies NS conditions ie.

$$\Sigma_a\, p(abcd|xyzw)=p(bcd|yzw) \text{ etc. ...}$$

Result. There exists an inequality implied by (i) and (ii) made of correlations ACD, ABD

$$S \leq 7$$

however quantum mechanics provides the value $S_Q \approx 7.2$!



[J. D. Blancal, S. Pironio, A. Acin, Y.-C. Liang, V. Scarani, N. Gisin, Nat. Phys. (2012)]

Describing a set Q: Semidefinite hierarchy and quantum correlations

Problem: Given probabilities { p(ab|xy) } how to verify their quantumness ?

Quantum probabilities: $p(ab|xy) = \langle\Psi|\, E'_{a,x} \otimes F'_{b,y}\, |\Psi\rangle$ or

$p(ab|xy) = \langle\Psi|\, E_{a,x}\ F_{b,y}\, |\Psi\rangle$ with orthogonal projectors $\{E_{a,x}\},\{F_{b,y}\}$

satisfying in addition $[E_{a,x}, F_{b,y}] = 0$

$(E_{a,x} = E'_{a,x} \otimes I,\ F_{b,y} = I \otimes F'_{b,y})$

The following matrix $$\Gamma_{ij} = \langle\Psi|\ (O_i)^\dagger O_j\, |\Psi\rangle$$

of the Gramm form $\Gamma_{ij} = \langle u_i|u_j\rangle$ has nonegative spectrum: $\Gamma \geq 0$

Semidefinite hierarchy and quantum correlations (II)

$$\Gamma_{ij} = \langle\Psi|\ (O_i)^\dagger O_j\ |\Psi\rangle \quad \Rightarrow \quad \Gamma \geq 0$$

Putting i = (a,x), j= (b,y) define

$$O_i = I\,,\ \underbrace{\overbrace{E'_{1,1}\,,\ \ldots,\ E'_{n,1}}^{\text{All Alice projectors}}}_{\text{1-st measurement of Alice}}\,,\ \ldots\ ,\ \underbrace{\overbrace{F'_{1,1}\,,\ \ldots,\ F'_{m,1}}^{\text{All Bob projectors}}}_{\text{1-st measurement of Bob}}\,,\ \ldots,$$

Since $E'_{a,x}\,,\ E'_{a',x} = \delta_{aa'} E'_{a,x}$, $F'_{b,y}\ F'_{b',y} = \delta_{bb'} F'_{b,y}$ (♦) and $[E'_{a,x}\,,\ F'_{b,y}] = 0$ (♦♦)

$$\Gamma_{0,(a,x)} = \langle\Psi|\ E'_{a,x}\ |\Psi\rangle = p(a|x) \qquad \Gamma_{(a',x),(a,x)} \overset{(\blacklozenge)}{=} \langle\Psi|\ E'_{a',x}\,E'_{a,x}\ |\Psi\rangle = \delta_{a,a'}\ p(a|x)$$

$$\Gamma_{0,(b,y)} = \langle\Psi|\ F'_{b,y}\ |\Psi\rangle = p(b|y) \qquad \Gamma_{(b,y),(b',y)} \overset{(\blacklozenge)}{=} \langle\Psi|\ E'_{b,y}\,E'_{b',y}\ |\Psi\rangle = \delta_{b,b'}\ p(b|y)$$

the same measurement

$$\Gamma_{(a,x),(a',x')} = \langle\Psi|\ E'_{a',x}\,E'_{a,x'}\ |\Psi\rangle = ? \qquad \Gamma_{(a,x),(a',x')} = \langle\Psi|\ E'_{a',x}\,E'_{a,x'}\ |\Psi\rangle = ?$$

different possibly noncommuting measurements

$$\Gamma_{(a,x),(b,x)} \overset{(\blacklozenge\blacklozenge)}{=} \Gamma_{(b,y),(a,x)} = \langle\Psi|\ E'_{a,x}\,F'_{b,x}\ |\Psi\rangle = p(ab|xy)$$

Semidefinite hierarchy and quantum correlations (III)

Example. **Alice** two settings (x,x'), n outcomes each .
Bob two settings (y,y'), m outcomes each.

$\Gamma =$

I	$E_{1,x}, \dots, E_{n,x}$	$E_{1,x'}, \dots, E_{n,x'}$	$F'_{1,y}, \dots, F_{m,y}$	$F_{1,y'}, \dots, F_{m,y'}$
1	$[p(a\|x)]_n$	$[p(a\|x')]_n$	$[p(b\|y)]_m$	$[p(b\|y')]_m$
	$\mathrm{diag}[p(a\|x)]_{n \times n}$	$[\ ?\ ]_{n \times n}$	$[p(ab\|xy)]_{n \times m}$	$[p(ab\|xy')]_{n \times m}$
		$\mathrm{diag}[p(a\|x')]_{n \times n}$	$[p(ab\|x'y)]_{n \times m}$	$[p(ab\|x'y')]_{n \times m}$
	... (h.c.)		$\mathrm{diag}[p(b\|y)]_{m \times m}$	$[\ ?\ ]_{m \times m}$
				$\mathrm{diag}[p(b\|y')]_{m \times m}$

many zeros on the block diagonal part

Observation.

Positivity condition $\Gamma \geq 0$ (ie. nonvegative eigenvalues)
is a necessary test of quantumness of **P**={p(ab|xy)}.
If adjusting (free) $[\ ?\ ]_{n \times n}$ parts to make Γ positive is **not possible**
$\Rightarrow$ **P** is **not quantum.**

Semidefinite hierarchy and quantum correlations (IV)

$$\Gamma = \begin{array}{c|c|c|c|c|}
I & E_{1,x}, \dots, E_{n,x} & E_{1,x'}, \dots, E_{n,x'} & F_{1,y}, \dots, F_{m,y} & F_{1,y'}, \dots, F_{m,y'} \\
\hline
1 & [p(a|x)]_n & [p(a|x')]_n & [p(b|y)]_m & [p(b|y')]_m \\
\hline
 & \mathrm{diag}[p(a|x)]_{n\times n} & [\,?\,]_{n\times n} & [p(ab|xy)]_{n\times m} & [p(ab|xy')]_{n\times m} \\
\hline
 & & \mathrm{diag}[p(a|x')]_{n\times n} & [p(ab|x'y)]_{n\times m} & [p(ab|x'y')]_{n\times m} \\
\hline
 & & & \mathrm{diag}[p(b|y)]_{m\times m} & [\,?\,]_{m\times m} \\
\hline
 & \text{h.c.} & & & \mathrm{diag}[p(b|y')]_{m\times m} \\
\hline
\end{array}$$

Semidefinite programme (SDP) to verify existence of positive Γ.

Minimise λ

subject to: (i) constraints above (via probabilites given { $p(ab|xy)$ })

(ii) $\Gamma - \lambda I \geq 0$

Test of quantumness

Remarks: Variational problem over ,,question marks'' **[?].**

SDP - standard task in computer science.

Constraints take into account that $p(a|x)=\Sigma_b p(ab|xy)$, $p(b|x)=\Sigma_a p(ab|xy)$.

Semidefinite hierarchy and quantum correlations (IV)

$\Gamma^{(0)} = I$

$\Gamma^{(1)}$ - $I \cup \{E_{a,x}\} \cup \{F_{b,y}\}$ (linear)

$\Gamma^{(2)}$ - $I \cup \{E_{a,x}\} \cup \{F_{b,y}\} \cup \{ \{E_{a,x} E_{a',x'}\} \cup \{E_{a,x} F_{,b,y}\} \cup \{F_{b,y} F_{b',y}\} \}$ (linear + quadratic)

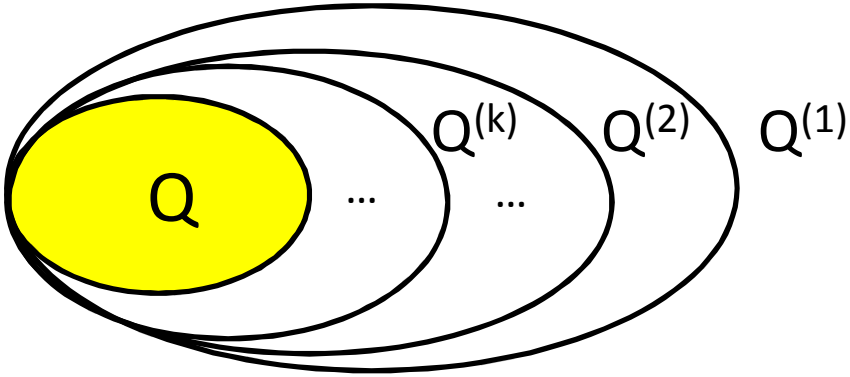
...

$\Gamma^{(k)}$ - $I \cup \{E_{a,x}\} \cup \{F_{b,y}\}$ ... (linear + quadratic + ... + k-th order)

Constraints: $[\Gamma^{(k)}]_{R,S} = [\Gamma^{(k)}]_{O,T} \Leftrightarrow R^{\dagger}S = O^{\dagger}T$ (with help of commutation relations)

Define sets

$Q^{(k)} = \{ \mathbf{P}: \mathbf{P} \in Q^{(k)} \Leftrightarrow \Gamma^{(k)} \geq 0 \}$

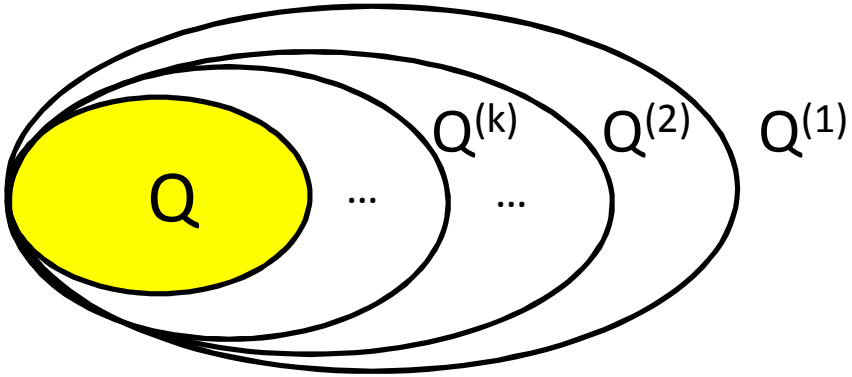


Problem: Is $P = \{ p(ab|xy) \}$ quantum ? In other words, are there state $|\Psi\rangle$ and measurements $\{E_{a,x}, F_{b,y}\}$, $[E_{a,x}, F_{b,y}] = 0$ such that

$$p(ab|xy) = \langle\Psi| E_{a,x} F_{b,y} |\Psi\rangle \quad ?$$

Semidefinite hierarchy and quantum correlations (IV)

$Q^{(k)} = \{ \mathbf{P}: \ \mathbf{P} \in Q^{(k)} \Leftrightarrow \Gamma^{(k)} \geq 0 \}$



Problem:
Is P = { p(ab|xy) } quantum ?

Theorem. $Q = \bigcap_{k=1}^{\infty} Q^{(k)}$ hence **P** is quantum $\Leftrightarrow$ $\Gamma^{(k)} \geq 0$ for any k.

Moreover if **P** comes from finitedimensional $|\Psi\rangle$, $\{E_{a,x}, F_{b,y}\}$ then there are stopping conditions to retrieve them at finite level so that

$$p(ab|xy) = \langle\Psi| \ E_{a,x} \ \ F_{b,y} \ |\Psi\rangle, \ \ [E_{a,x}, F_{b,y}] = 0$$

with product (!) representation $E_{a,x} = E'_{a,x} \otimes I$, $F_{b,y} = I \otimes F'_{b,y}$

[M. Navascues, S. Pironio, A. Acin, Phys. Rev. Lett. (2007); New J. Phys. (2008)]

The case of dim = ∞ related to B. Tsirelson problem:

$[E_{a,x}, F_{b,y}] = 0 \Leftrightarrow E_{a,x} = E'_{a,x} \otimes I$, $F_{b,y} = I \otimes F'_{b,y}$ (true for dim < ∞)

Generalisation to the case of Bell inequalities

Observation. The construction can be extendeed to Bell inequalites since any value of Bell inequality can be written as :

Maximise $B = \Gamma^{(n)} Q$ (Q indicator matrix defining the inequality)

(i) constraints on Γ (via probabilites given { p(ab|xy) })

(ii) $\Gamma^{(n)} \geq 0$

Saturation checked by the so called dual problem.

Sometimes quantum value reproduced at the first hierarchy $\Gamma^{(n)}$.

Theorem. [Tsirelson (1987)] $A_1,\ldots,A_n$; $B_1,\ldots,B_n$ with eigenvalues from [-1,1] then the correlation functions satisfy

$$\langle\psi|\, \mathbf{A_i} \otimes \mathbf{B_j} \,|\psi\rangle = u_i\, v_j$$

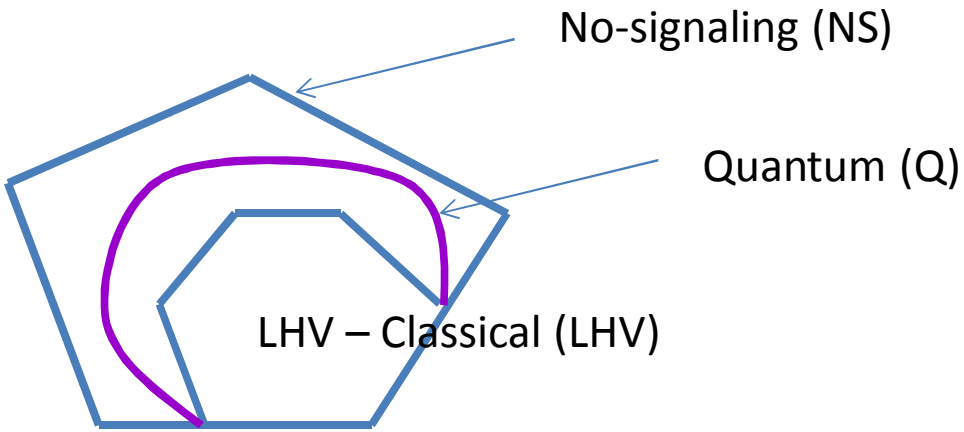
for some unit vectors $\mathbf{u} = [u_1,\ldots,u_n] \in R^n$, $\mathbf{v} = [v_1,\ldots,v_n] \in R^n$.

Observation. For any ineqality based on correlations above quantum value reproduced at the first level ($\Gamma^{(1)}$) .

[S. Wehner, Phys. Rev. A (2006)]

Example. $\langle \mathbf{B}\rangle_\psi = \langle\psi|\, \mathbf{A_1} \otimes \mathbf{B_1} + \mathbf{A_1} \otimes \mathbf{B_2} + \mathbf{A_2} \otimes \mathbf{B_1} - \mathbf{A_2} \otimes \mathbf{B_2} \,|\psi\rangle$, $(\mathbf{A_i})^2 = (\mathbf{B_i})^2 = 1$

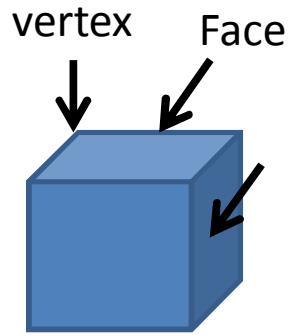
General issue – what is a geometry of the sets ?



Convex sets

NS and LHV are convex polytopes (compact convex set with a finite numbers of extreme points)

Q is not a polytope



(n-1) Face
- Facet

,,Planar'' boundaries of the polytopes

Interesting paradox with a facet

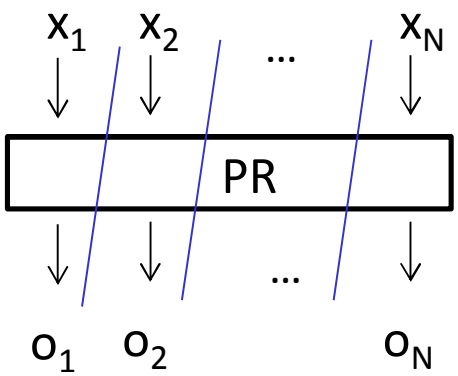
For $N \geq 3$ there is LHV facet which is a Q facet but is not a NS facet.

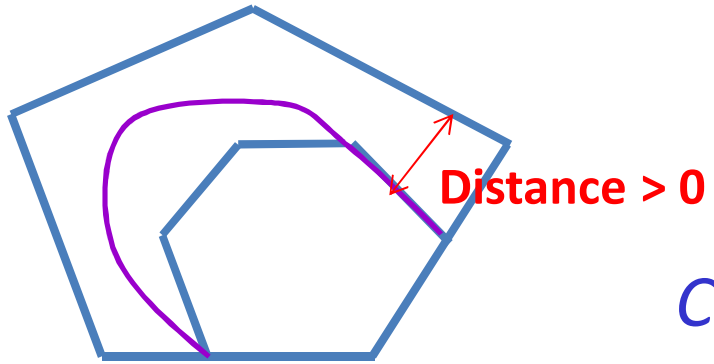
Gess your neighbour's input (GYNI) game

$\mathbf{x} = [x_1,\ldots,x_N]$, $x_i \in \{0,1\}$

$\mathbf{o} = [o_1,\ldots,o_N]$, $o_i \in \{0,1\}$

$N \geq 3$





Case N=2:

an open question

$$B = \Sigma_{\mathbf{ox}}\ p(\mathbf{x})\ \chi(\mathbf{o}, \mathbf{x}: o_i = x_{i+1})\ p(\mathbf{o}|\mathbf{x}) = \Sigma_{\mathbf{x}}\ p(\mathbf{x})\ p(o_i = x_{i+1}|\mathbf{x})$$

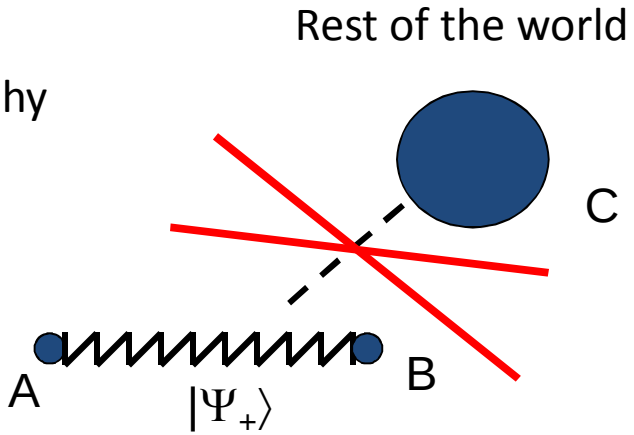
$$C_{LHV} = C_Q = \max_{\mathbf{x}} [p(\mathbf{x}) + p(\mathbf{x}')] \qquad x_i' = x_i \oplus 1 \text{ (negation)}$$

For $p(\mathbf{x}) = 2^{-(N-1)}$ with $x_1 \oplus \ldots \oplus x_N = 0$ this gives

$$C_{LHV} = C_Q = 2^{-(N-1)} < C_{NS} = (4/3)\ 2^{-(N-1)}$$

Extremal points and the vertices issue

- **Extremal points** are very important cryptografically.
  In quantum mechanics entanglement based cryptography bases on **extremality of singlet.**
- **Extremality of singlet is an „extremal" expression of quantum monogamy: if A is maximally entangled with B then it can not be entangled with C at all.**



Sequrity against quantum. Maximal entanglement is enough from the perspective of quantum mechanics to ensure **security** or **certified randomness**.

What about security against postquantum ?
Namely, the state statistica might be not correlated with any quantum state but correlated with some post-quantum (no-signaling) adversary system.

Observation.
Possible remedy - quantum statistics reproducing extremal points of the NS polytope.

Do they exist ???

Monogamy of no-signaling correlations (I)

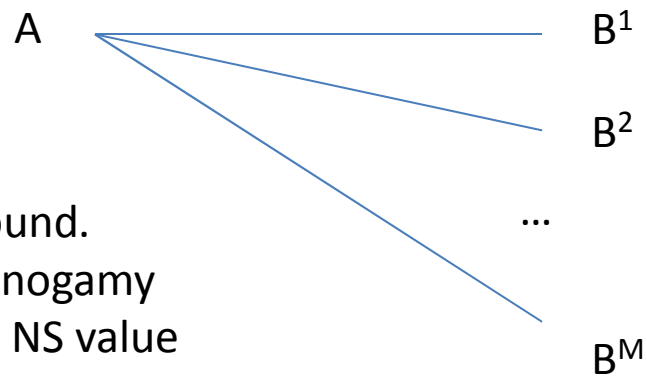
[Terhal at al. PRA 2003, Pawlowski Bruckner PRL 2009]

1) Bipartite Bell inequality with (i) settings m_A, m_B (ii) outcomes d_A, d_B

$$\mathcal{B}_{AB} := \mathbb{B}.\mathbb{P} \leq \mathbf{R_{LHV}}(\mathbb{B})$$

2) Considered M+1 multipartite no-signaling box
$P(a,b_1,\ldots,b_M|xy_1,\ldots,y_M)$ that generates M bipartite boxes $P(ab_i|xy_i)$.
The monogamy relation is:

$$\Sigma_{i=1}^{M} \mathcal{B}_{\square\square\square} \leq M\mathbf{R_{LHV}}(\mathbb{B})$$



Remark.
(i) Smaller M – tighter the monogamy bound.
(ii) When the Bell matrix positive the monogamy relation leads to an upper bound on the NS value

$$\mathbf{R_{NS}}(\mathbb{B}) \leq M\mathbf{R_{LHV}}(\mathbb{B}).$$

Question: what is M for the specific Bell inequalities ?

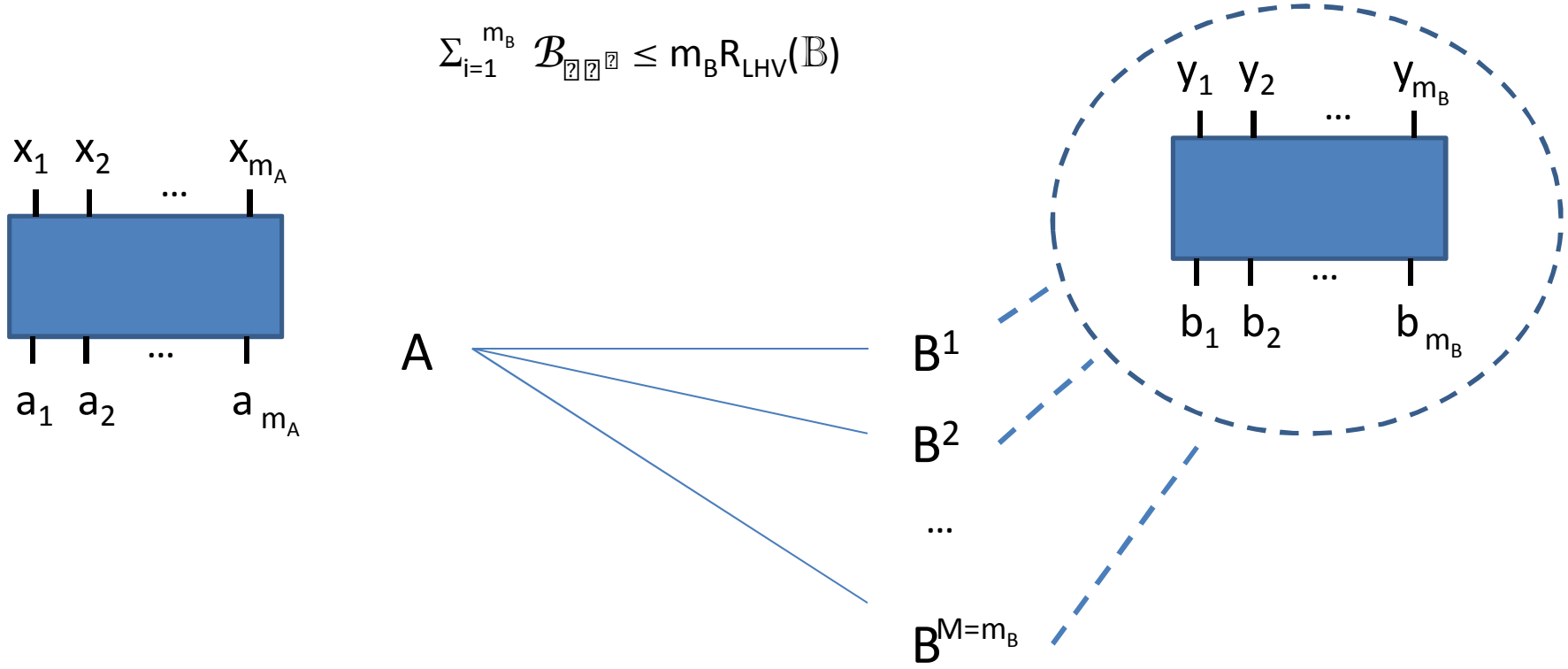
Monogamy of superquantum correlations (II)

[Terhal at al. PRA 2003, Pawlowski Bruckner PRL 2009]

Thm. For bipartite inequality $\mathcal{B}_{AB} := \mathbb{B}.\mathbb{P} \leq R_L(\mathbb{B})$ with (i) settings m_A, m_B (ii) outcomes d_A, $d_B = m_B$ the monogmy relation is satisfied for $M = m_B$.

(Number of Bobs equal to the number of settings of each of them)

$$\Sigma_{i=1}^{m_B} \mathcal{B}_{\square\square\square} \leq m_B R_{LHV}(\mathbb{B})$$

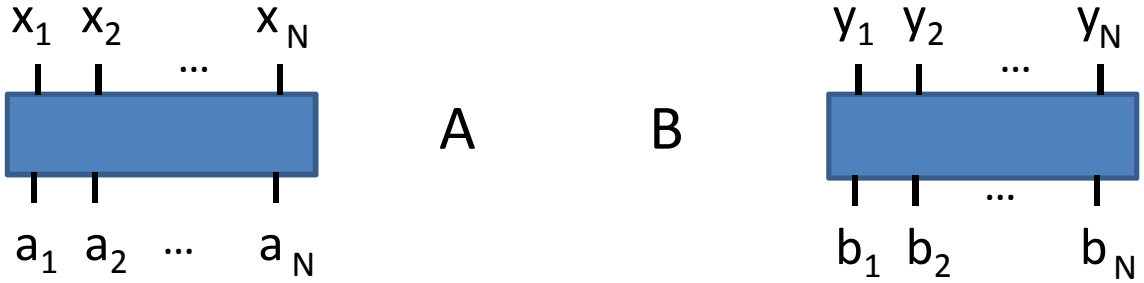


Chain inequality (I)

[Braunstein & Caves PRL 1988]

Settings: $m_A = m_B = N$

Outcomes: $d_A = d_B = 2$

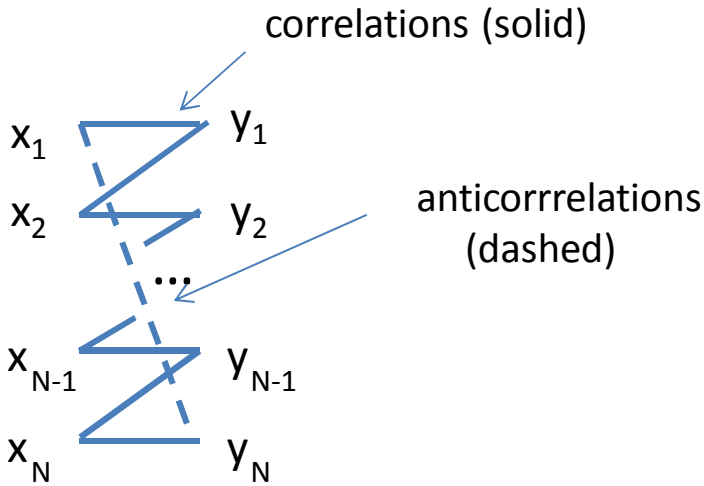


Example.

Indicator matrix for N=3. Probability matrix p(x,y) arbitrary (usually taken uniform).

x \ y	a \ b	0		1		2	
		0	1	0	1	0	1
0	0	1					1
	1		1			1	
1	0	1		1			
	1		1		1		
2	0			1		1	
	1				1		1

In terms of settings:



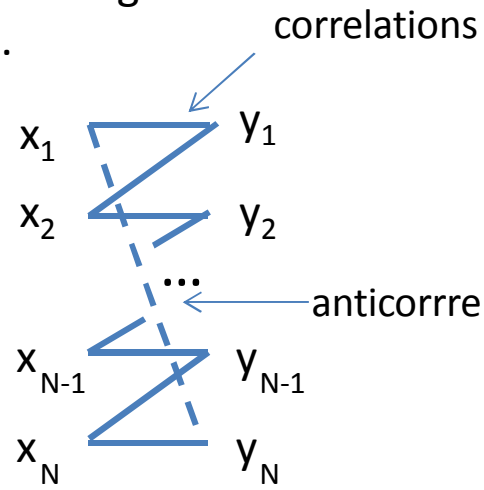
Standard monogamy $\Sigma_{i=1} \mathcal{B}_{\square\square\square} \leq NR_{LHV}(\mathbb{B})$

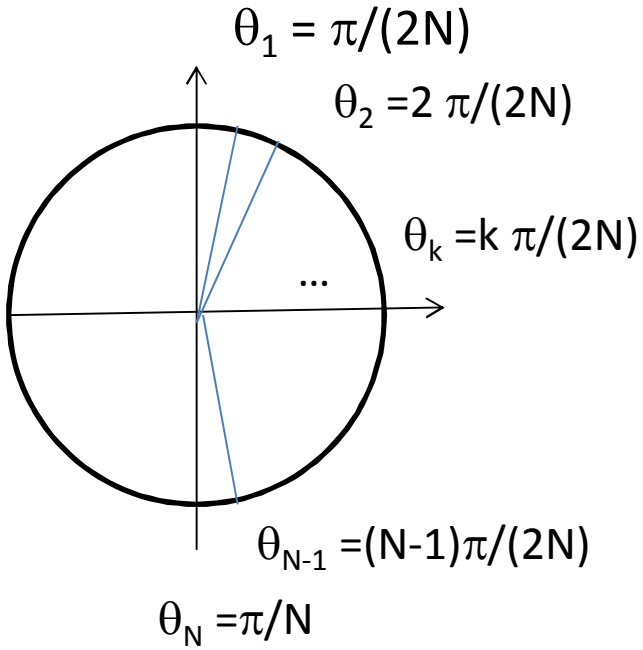
Is there a chance for any stronger relation ?

Chain inequality

Next neighbours settings only with perfect correlation. θ_N and θ_1 closing the chain with antycorrelation.

$|\Psi\rangle=(|0\rangle|0\rangle+|1\rangle|1\rangle)/\sqrt{2}$





Probabilities of winning:

$C_{LVH} = 1 - 1/2N$

$C_Q = 1 - \sin^2(\pi/4N)$

$C_{NS} = 1$

It is better to compare probabilities of ,,loosing the game'':

$\beta_{LVH} = 1/2N$

$\beta_Q = \sin^2(\pi/4N)$

$\beta_{NS} = 0$

$$\beta_Q/\beta_{LVH} \xrightarrow{N\to\infty} 0$$

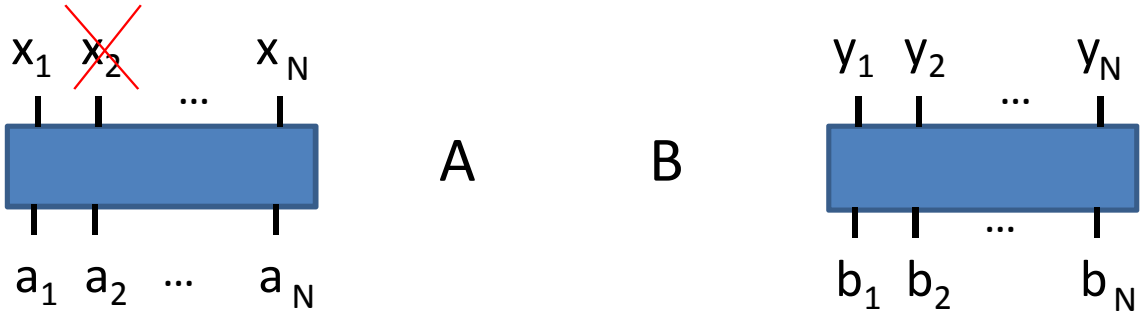
Quantum value approaches NS limit faster than LHV

Chain inequality (II)

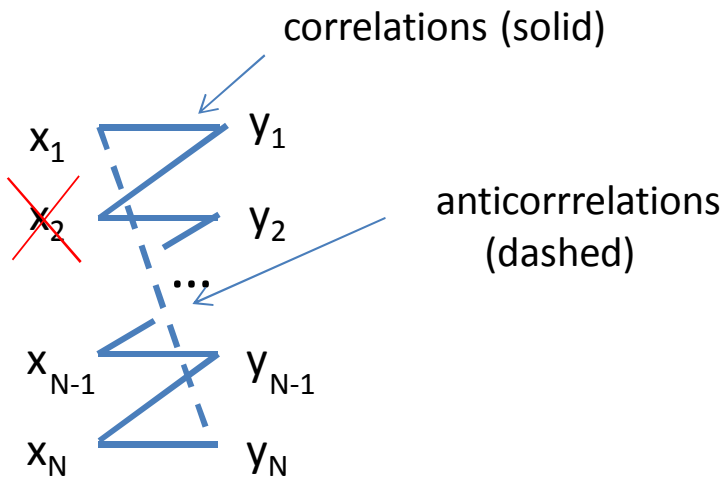
[Braunstein & Caves PRL 1988]

Settings: $m_A = m_B = N$

Outcomes: $d_A = d_B = 2$



If only 1 setting is removed the inequality becomes classical – *chain is „broken'': and there is no contradictory constraints on classical value.*



Contradiction number with respect to Bob

[R. Ramanathan, P.H. Phys. Rev. Lett. (2014)]

Nontrivial inequality: $\mathcal{B}_{AB} := \mathbb{B}.\mathbb{P} \leq R_{LHV}(\mathbb{B}) < R_{NS}(\mathbb{B})$ (*)

$$\mathbb{B}.\mathbb{P} = \sum_{i=1}^{m_A} \sum_{j=1}^{m_B} \sum_{a=1}^{d_A} \sum_{b=1}^{d_B} p(x,y)B'(a,b,x,y)P(ab|xy)$$

Define new inequality $\mathcal{B}'_{AB} := \mathbb{B}'.\mathbb{P} \leq R_{LHV}(\mathbb{B}') \overset{?}{<} R_{NS}(\mathbb{B}')$ (**)

$$\mathbb{B}'.\mathbb{P} := \sum_{i=1}^{m_A} \sum_{j=1}^{m_B - C} \sum_{a=1}^{d_A} \sum_{b=1}^{d_B} p(x,y)B'(a,b,x,y)P(ab|xy)$$

and all its variants up to permutations of Bob settings.

Df. Contradiction number C of the inequality (*) with respect to Bob is the minimal ,,deficit'' in B settings that makes the inequality (**) trivial

$$\mathcal{B}'_{AB} := \mathbb{B}'.\mathbb{P} \leq R_{LHV}(\mathbb{B}') = R_{NS}(\mathbb{B}')$$

Stronger monogamy relation for binary XOR games

[R. Ramanathan, P.H. PRL in press (2014)]

Settings: $m_A = m_B = N$

Outcomes: $d_A = d_B = 2$ $\quad \mathcal{B}^{\oplus}_{AB} := \mathbb{B}^{\oplus}.\mathbb{P} \leq R_{LHV}(\mathbb{B}) < R_{NS}(\mathbb{B})$

$$\mathbb{B}^{\oplus}.\mathbb{P} = \sum_{i=1}^{m_A} \sum_{j=1}^{m_B} \sum_{a=1}^{d_A} \sum_{b=1}^{d_B} p(x,y)B'(a\oplus b,x,y)P(ab|xy)$$

(dependence on XOR function of the outcomes, chain inequality included).

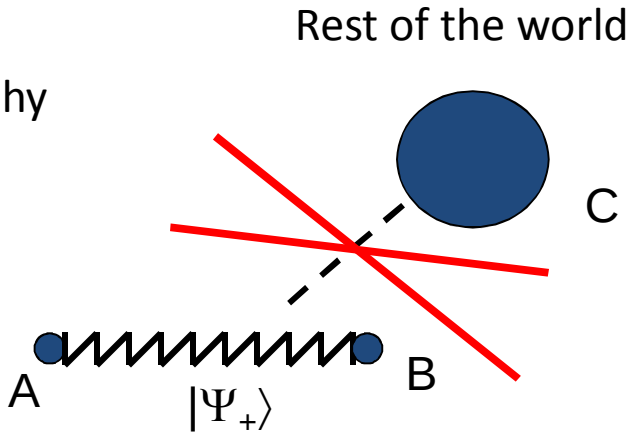
$$\boxed{\sum_{i=1}^{C+1} \mathcal{B}^{\oplus}_{\square\square\square} \leq (C+1)R_{LHV}(\mathbb{B})}$$

which for chain provides the inequality (since for it C=1):

$$\boxed{\mathcal{B}^{(chain,\,N)}_{AB} + \mathcal{B}^{(chain,\,N)}_{AC} \leq 2R_{LHV}(\mathbb{B}^{(chain,\,N)})}$$

Extremal points and the vertices issue

- **Extremal points** are very important cryptografically.
  In quantum mechanics entanglement based cryptography happens due to **extremality of singlet.**
- **Extremality of singlet is an „extremal" expression of quantum monogamy: if A is maximally entangled with B then it can not be entangled with C at all.**



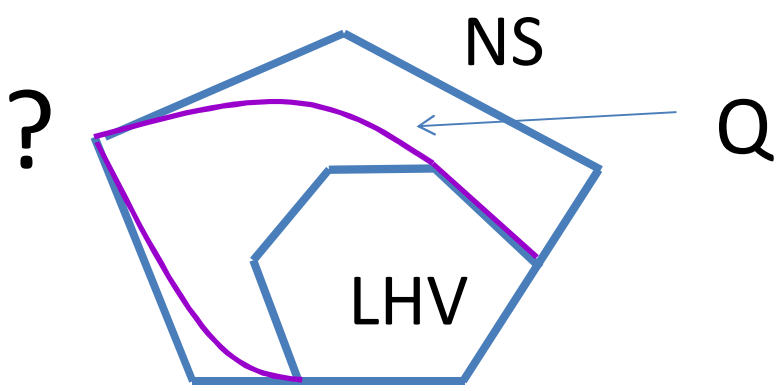
Sequrity against quantum. Maximal entanglement is enough from the perspective of quantum mechanics to ensure **security** or **certified randomness**.

What about security against postquantum = no-signaling?
Namely, the state statistics might be not correlated with any quantum state but correlated with some post-quantum (no-signaling) adversary system.

Immediate observation.
Possible remedy - quantum statistics reproducing extremal points of the NS polytope.

Do they exist ?

Question: are there nontrivial Q vertices in NS ?



Nontrivial = outisde of LHV

Connection of boxes with orthogonality graphs.

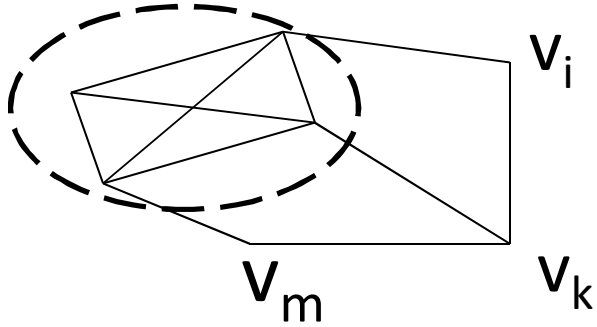
G - orthonormal representation of the box P $\Leftrightarrow$
vertices – orthonormal vectors from the measurements

$v_i \perp v_k$

$v_k \perp v_m$

$v_i \not\perp v_m$

Clique – all vertices connected
- all vectors orthogonal



i = (a,b,x,y), k= (a',b',x',y')
Orthogonality :
(x=x' and $a \neq a'$) or (y=y' and $a \neq a'$) .

TH(G) = { ,,unnormalised boxes'' P: $p=|\langle v_i \mid \psi\rangle|^2$, s.t. $|v_i\rangle$ ortonorm. repr., ψ normalised } [Grotshel, Lovash, Schrijver, J.Comb. Theory (1986)]

Normalisation and NS $\rightarrow$ some cliques of the graph.

TH_c(G) = {P: P $\in$ TH(G), P satisfies normalisation + NS }

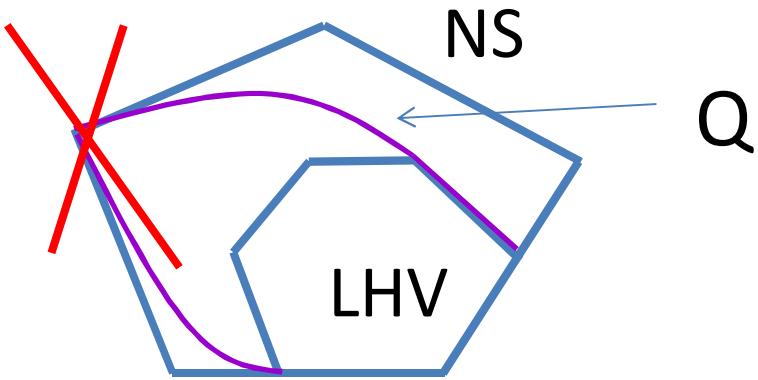
Theorem:
(i) $TH_c(G)=Q^{(1+AB)} \subset Q^{(1)} \subset Q$ (superset of quantum set Q)
(ii) All nontrivial NS vertices outside of $TH(G) \subset TH_c(G)$

Nontrivial vertices outside of the superset of Q $\Rightarrow$ they are outside of Q

[R. Ramanathan, J. Tuziemski, M. Horodecki, P. H. arxiv.1410.0947]

Question: are there nontrivial Q vertices in NS ?

Nontrivial = outiside of LHV



Negative answer $\Rightarrow$ limitations of possible strategies for secure randomness or cryptography against NS evesdropper. Quantum extremal point (singlet) strategy can not be repeated on the NS ground.

Problem of weak randomness amplification

Natural generalisation of sequence of biased coins $p_+ : p_-$ $p_\pm = ½ \pm \epsilon$

Smaller ϵ
- better.

Df. Santha-Vazirani source (called ϵ-SV source).
The source of an (arbitrary long) string of bits $\{x_1, \ldots, x_n\}$
s. t. conditioning upon its past leaves the bit ϵ-free:

$$½ - \epsilon \leq p(x_i \mid x_{i-1}, \ldots, x_1) \leq ½ + \epsilon$$

Theorem.- [M. Santa, U. Vazirani, (1984)]
There is no classical deterministic function that would produce from ϵ-SV source the bit that is ϵ'-free with $\epsilon' < \epsilon$.

For characterisation of extremal poits of ϵ-SV see
[A. Grudka, Andrzej, K. Horodecki, M. Horodecki, P.H., M. Pawłowski, R. Ramanathan Phys. Rev. A 90, 032322 (2014)]

Problem of randomness amplification against NS evesdropper

Eve

Alice $\{ p(\mathbf{ab}e|\mathbf{xy}w) \}$ Bob

$$\frac{1}{2} - \epsilon \leq p(x_i \mid x_{i-1}, \ldots, x_1, e, w) \leq \frac{1}{2} + \epsilon$$

NS box with quantum
$\{ p(\mathbf{ab}|\mathbf{xy}) \}$

ϵ-SV source: input ϵ-free-randomness

Pr ≈ 1

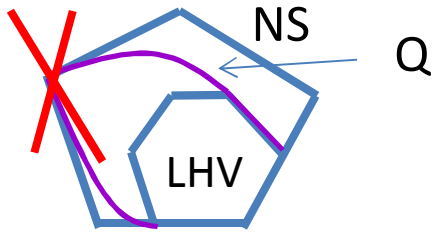
$$\frac{1}{2} - \epsilon' \leq p(s|e,w) \leq \frac{1}{2} + \epsilon'$$

e - single bit (Eve's guess)

output ϵ'-free random bit
ϵ' arbitrary close to 0.

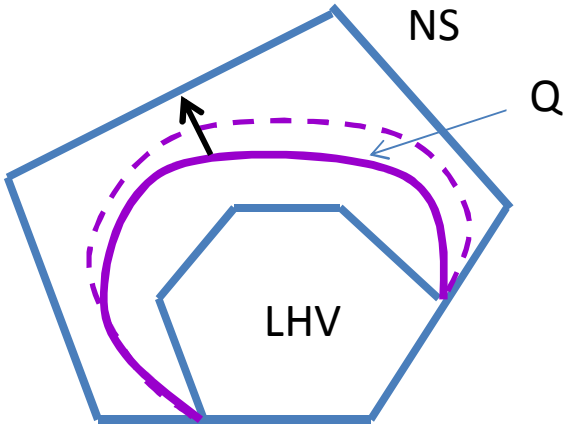
[R. Colbeck, R. Renner, Nat. Phys. (2012)]

Problem of randomness amplification against NS evesdropper



That option impossible (only recently proven). Intuitively it is clear that we have at least approach the boundary (can be formally proven).

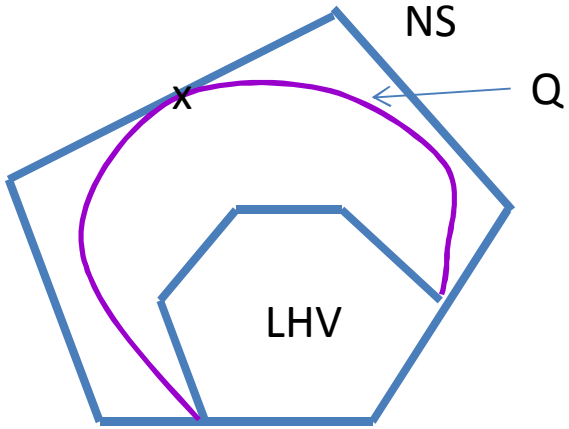
One option:



Approaching the boundary.

[R. Colbeck, R. Renner, Nat. Phys. 2012]
Pioneering. 2 qubit chain inequality. Problem - unbounded increase of no. of settings. Not universal (does not apply to weak randomness).

Another option:

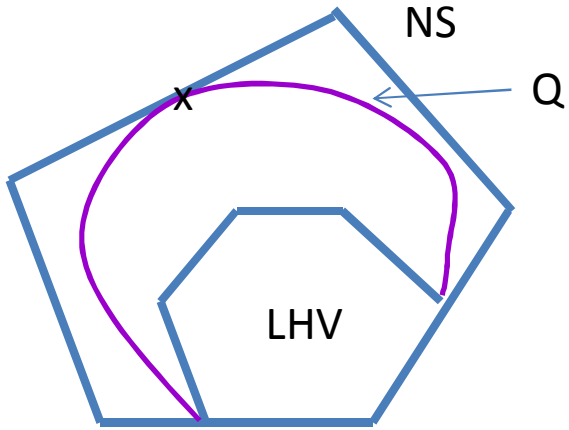


Tangent to the boundary from the very beginning ie. acheives maximal NS value.

[R. Gallego, et al. Nature Comm. (2013)]
5 qunits GHZ paradox. Problem – unbounded no. of devices.

Both results are not noise tolerant.

Problem of randomness amplification against NS evesdropper



Tangent to the boundary from the very beginning ie. acheive maximal NS value.

Solution with 4-qubit GHZ
Finite no. of settings and devices, noise tollerance.
Introduces a new version of quantum de Finetti theorem.

[F. G.S.L. Brandao, R. Ramanathan, A. Grudka, K. Horodecki, M. Horodecki, P. H., T. Szarek, H. Wojewodka , 1310.4544]

Solution with 4-ququarts (variant of GHZ paradox for two parites) solution. finite no. of settings and devices, tollerates noise. Based on graphs approach to quantum contextuality.

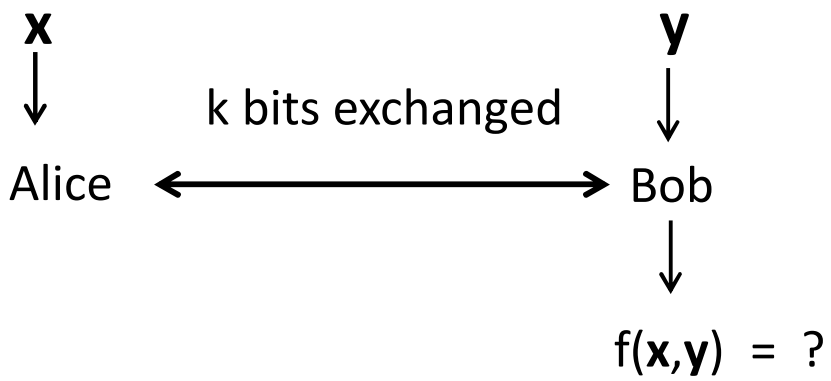
[R. Ramanathan, F. G.S.L. Brandão, K. Horodecki, M. Horodecki, P. H, H. Wojewódka, arXiv:1504.06313]

Communication complexity

General problem:

bit strings $\mathbf{x} = [x_1,\ldots,x_n]$, $x_i \in \{0,1\}$, $\mathbf{y} = [y_1,\ldots,y_n]$, $y_i \in \{0,1\}$

Boullean function $f(\mathbf{x},\mathbf{y})$, $f : \{0,1\}^{x\,n} \times \{0,1\}^{x\,n} \rightarrow \{0,1\}$



Deteministic variant: communication complexity (CC) of the function f is

$C(n) = k^*(n) = \min$ k such that Bob can compute $f(\mathbf{x},\mathbf{y})$ correctly }

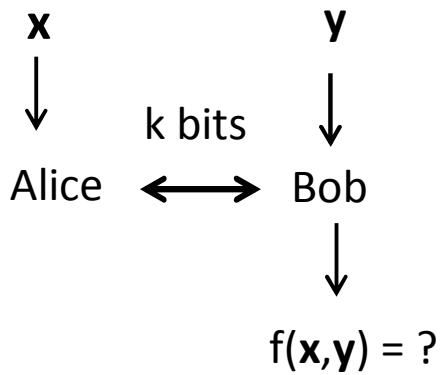
Probabilistic variant (with bounded bias):

CC of the function f is $C(n) = k^*(n) = \min$ k such that Bob can compute $f(\mathbf{x},\mathbf{y})$ correctly with probability

$$p=1/2 + \varepsilon \quad \text{(with } \varepsilon \text{ independent on n).}$$

Trivialisation of communication complexity by NS correlations (I)

$\mathbf{x} = [x_1,\ldots,x_n]$, $x_i \in \{0,1\}$, $\mathbf{y} = [y_1,\ldots,y_n]$, $y_i \in \{0,1\}$



Task: Calculate deterministically Inner Product function

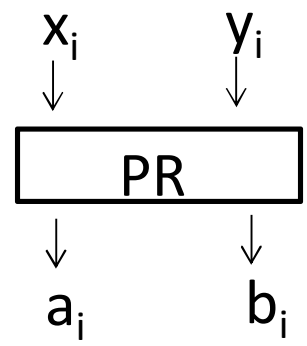
$$f_{IP}(\mathbf{x},\mathbf{y}) = \oplus_i x_i\, y_i = x_1\, y_1 \oplus x_2\, y_2 \oplus \ldots \oplus x_n\, y_n$$

Classically: Complex problem ie. $C(f_{IP})$ =min k = n (A must sent all her bits to B)

No-signaling theory: What is complexity $C_{PR}(f_{IP})$ if A & B use n PR boxes ?

$$f_{IP}(\mathbf{x},\mathbf{y}) = x_1\, y_1 \oplus \ldots \oplus x_n\, y_n = a_1 \oplus b_1 \oplus \ldots \oplus a_n \oplus b_n =$$

$$= (a_1 \oplus \ldots \oplus a_n) \oplus (b_1 \oplus \ldots \oplus b_n) = a' \oplus b'$$



$$a_i \oplus b_i = x_i\, y_i$$

Surprising solution: A & B use PR boxes n times.
each of them calculates sum of outputs - a', b'.
Finally A sends a' to B who calculates $a' \oplus b' = f_{IP}(\mathbf{x},\mathbf{y})$

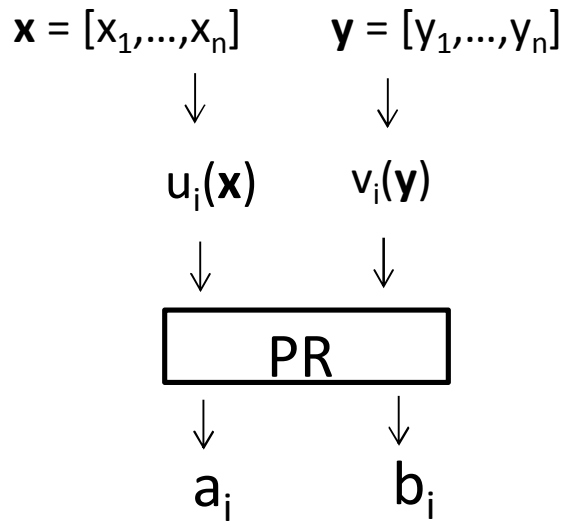
$C_{PR}(f_{IP})$ of Inner Product function is equal to 1 bit (a') of communication !

Trivialisation of communication complexity by NS correlations (II)

General question. What about other functions f(**x**,**y**) ?
What are their communication complexities if A & B can share n PR boxes ?

Fact. Any Bollean function f_n (**x**,**y**) **can be written as Inner Product function of two N-bit strings (N = 2^n)** **u(x)** = $[u_1(\mathbf{x}),\ldots,u_N(\mathbf{x})]$, **v(x)** = $[v_1(\mathbf{x}),\ldots,,\ldots,v_n(\mathbf{x})]$
with $u_i(\mathbf{x})$, $v_i(\mathbf{x})$ being binary polynomials of the original arguments.

$$f_n(\mathbf{x},\mathbf{y}) = u_1(\mathbf{x})\, v_1(\mathbf{y}) \oplus \ldots \oplus u_N(\mathbf{x})\, v_N(\mathbf{y})$$



$$a_i \oplus b_i = u_i(\mathbf{x})\, v_i(\mathbf{y})$$

Virtually the same strategy gives the same result $C(f_n)=1$
Only difference: $u_i(\mathbf{x})$, $v_i(\mathbf{y})$ must be calculated locally before using PR boxes.

Theorem. Communication complexity of any Bollean function f with assistance of PR boxes is trivial and equal to 1 bit.

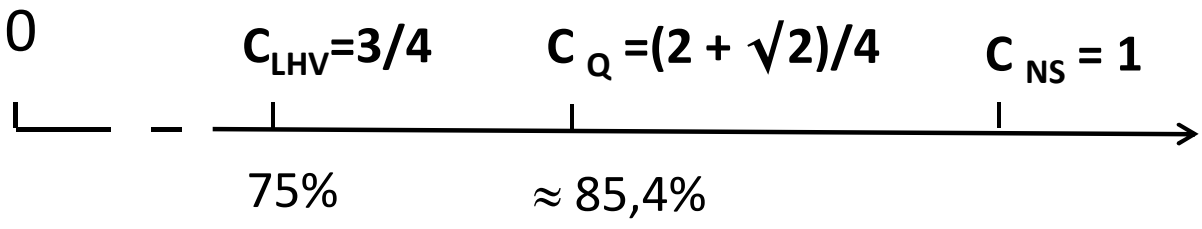
[W. van Dam, Ph. D. thesis, Oxford (2000)]

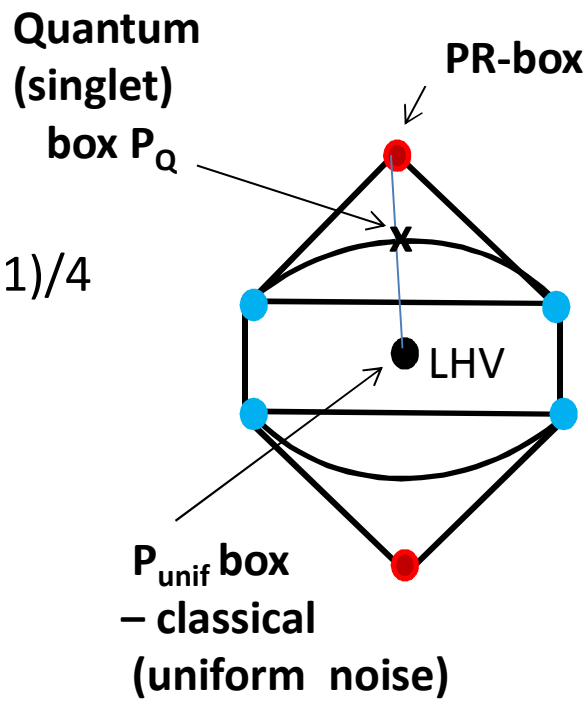
When CC is probabilistically not trivial ?

Convex combination $\mathbf{P} = q\,\mathbf{PR} + (1-q)\,\mathbf{P}_{unif}$

Bell value B - **probability of simulation of PR box**

$B^{sim}(\mathbf{P}) = 1/4\ \Sigma_{abxy}\ \chi(a,b,x,y:\ a \oplus b = x\,y)\ p(a,b|x,y) = (3q+1)/4$





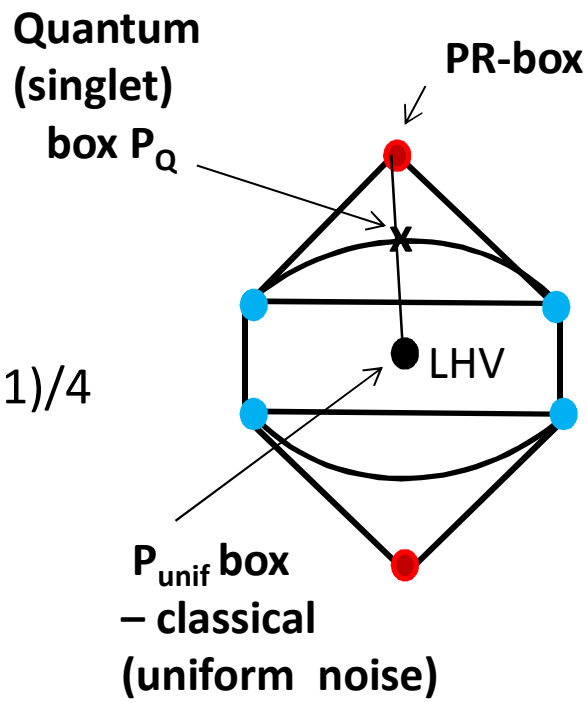
Problem. How big should be B^{sim} to make CC of any Bollean $f_n(\mathbf{x},\mathbf{y})$ probabilistically trivial ?

Answer. If only $B(P) \geq (3+\sqrt{6})/6 \approx 90.8\%$ then arbitrary Bollean function $f_n(\mathbf{x},\mathbf{y})$ can be calculated with probability $p \geq ½ + \varepsilon$ ie. is probabilistically computationally trivial.

[G. Brassard, H. Buhrman, N. Linden, A. A. Methot, A. Tapp, F. Unger, Phys. Rev. Lett. (2006)]

When CC is probabilistically not trivial ?

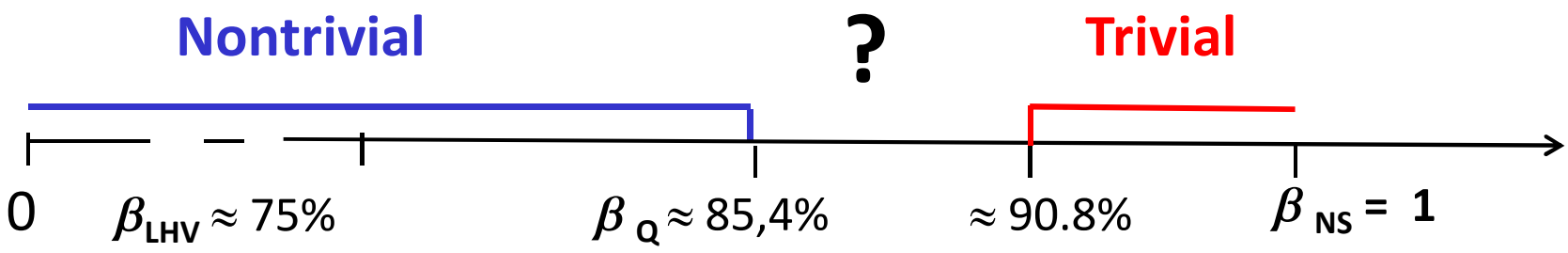
Convex combination: $\mathbf{P} = q\,\mathbf{PR} + (1-q)\,\mathbf{P}_{unif}$



Bell value B^{sim} - **probability of simulation of PR box**

$$B^{sim}(\mathbf{P}) = 1/4\ \Sigma_{abxy}\ \chi(a,b,x,y:\ a \oplus b = x\,y)\ p(a,b|x,y) = (3q+1)/4$$

Probabilistic communication complexity



[G. Brassard, H. Buhrman, N. Linden, A. A. Methot, A. Tapp, F. Unger, Phys. Rev. Lett. (2006)]

Physically (or philosophically) motivated principles reducing NS (no-signaling) set

General idea: make NS it as quantum as possible.

Remark. If something is left despite all the effort, may be it is physical ?

Principle: (NTCC) No trivial communication complexity in any physical theory.

Not known whether the result can be tightened to reproduce threshold betwen quantum and non-quantum NS boxes.

[G. Brassard, H. Buhrman, N. Linden, A. A. Methot, A. Tapp, F. Unger, Phys. Rev. Lett. (2006)]

Physically (or philosophically) motivated principles reducing NS (no-signaling) set

Principle: (ML) Macroscopic locality. Coarse-grained (macroscopic) measurement result on N independent composite systems should admit local description in any physical theory in the limit $N \to \infty$.

Mathematically it turnes our that any box P satisfies

$$P \in ML \iff P \in Q^{(1)} \quad \text{(first hierarchy)}$$

[M. Navascues, H. Wunderlich, Proc. Roy. Soc. Lond. (2009)]

Physically (or philosophically) motivated principles
reducing NS (no-signaling) set

Random access code ,,at a distance'' with help of PR box

Alice

$a_0, a_1 \in \{0,1\}$

Bob

$i = 0, 1$ (Alice bit index)

$p(i) = ½$ (random choice)

$x = a_1 \oplus a_0$

$y = i$

$a_i = ?$

PR

$a \oplus b = x\,y = i\,(a_1 \oplus a_0)$

a

b

$s = a_0 \oplus a$ $\longrightarrow$ $s \oplus b = a_i$

$\underbrace{s \oplus b}_{a_0 \oplus i\,(a_1 \oplus a_0)}$

[W. van Dam, Ph. D. thesis, Oxford (2000)]

Physically (or philosophically) motivated principles reducing NS (no-signaling) set

Alice $\xrightarrow{\quad m \quad}$ Bob $i = 0, 1, \ldots, n$ (Alice bit index variable Z)

$a_0, a_1, \ldots, a_n \in \{0,1\}$

$\downarrow$ $p(i) = 1/n$ (random choice)

(random, independent variables: A_i)

b (guess, variable B)

Principle: (IC) Information casuality.
The sum of conditional correlations of Bob's guess with Alice not exceed number of classical bits trensferred.

$$\sum_{i=1}^{n} I(A_i : B \mid Z = i)$$

The above perfectly reproduces quantum vs NS treshold on mixture of PR boxes with uniform noise.

[M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, M. Zukowski, Nature 461, 1101 (2009)]

Physically (or philosophically) motivated principles reducing NS (no-signaling)

Events $(\mathbf{a}|\mathbf{x})$ and $(\mathbf{a}'|\mathbf{x}')$ are locally orthogonal (LO) iff they contain $x_i = x_i'$, but $a_i = a_i'$

Principle: (LO) Local orthoginality

$$\sum_{(\mathbf{a}|\mathbf{x}) \in \{\text{set of mutually LO events}\}} p(\mathbf{a}|\mathbf{x}) \leq 1$$

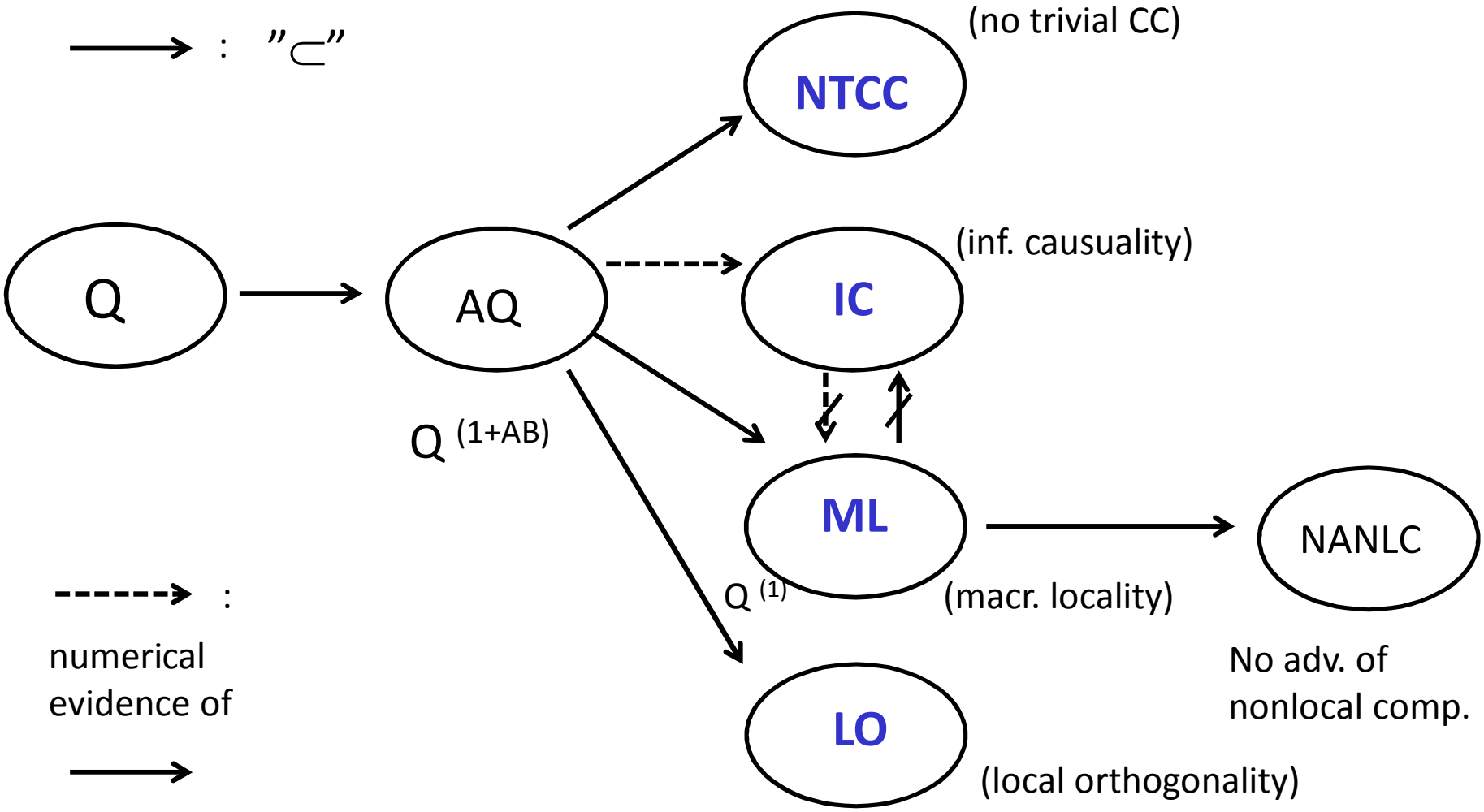
$$p(000|000) + p(110|011) + p(011|001) + p(101|110) \leq 1$$

This is one of the GYNI inequalities – violated by NS up to 4/3.

For bipartite systems on single instance eiwuivalent to NS + nomalisation)

[T. Fritz, A. B. Sainz, R. Augusiak, J. B. Brask, R. Chaves, A. Leverrier, A. Acín, Nature Communications 4, 2263 (2013)]

Relations among some postulated principles



M. Navascues et al., 1403.4621, Nat Comm (2014).

Fundamental property: complementarity

Werner Heisenberg
(1901-1976)

$$\Delta q \, \Delta p \geq \hbar/2$$

HEISENBERG UNCERTAINTY PRINCIPLE

"One may view the world with a p-eye and one may view it with a q-eye, but if one opens both eyes simultaneously, one than gets crazy."

W. Pauli in his letter to W. Heisenberg
(dated 19 October 1926)

Wolfgang Pauli
(1900-1958)

$$H(q) + H(p) \geq 1 + \ln\pi$$

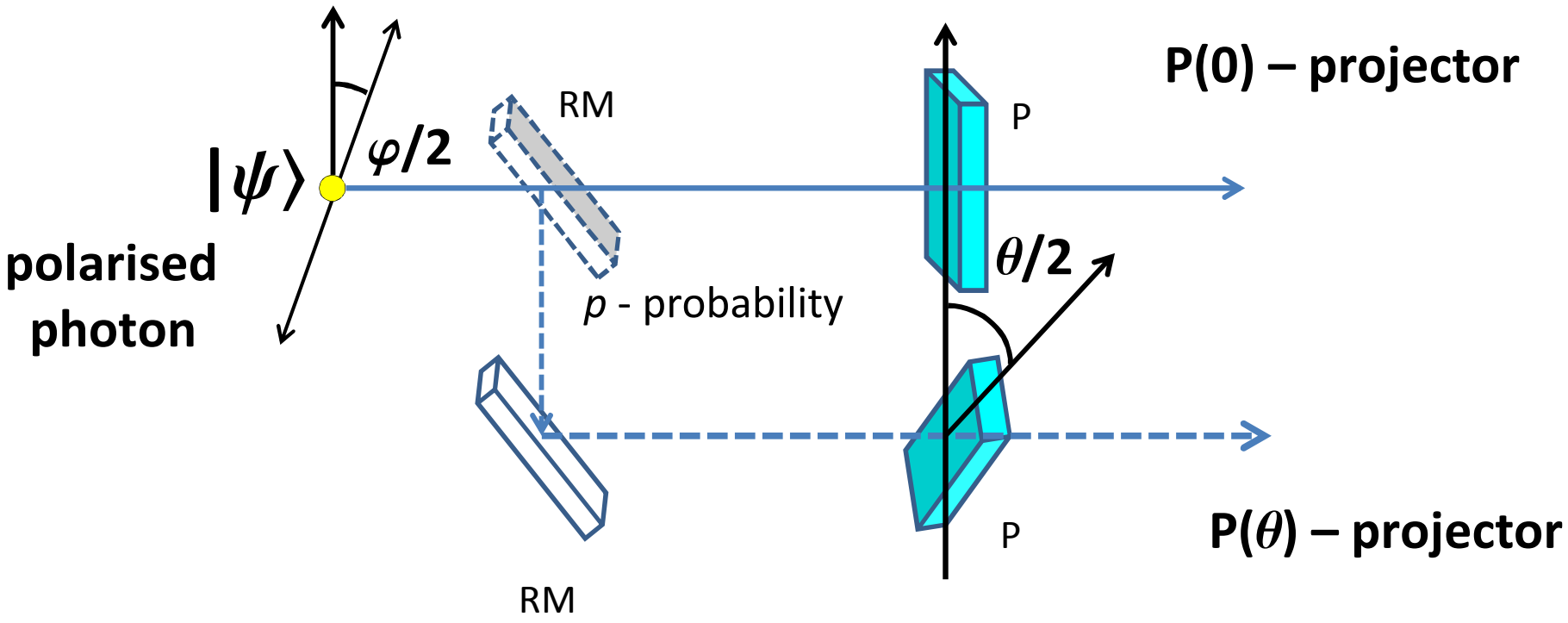
I. Białynicki-Birula, J. Mycielski, Comm. Math. Phys. 44, 129 (1975)

$$H(\sigma_x) + H(\sigma_z) \geq \log 2$$

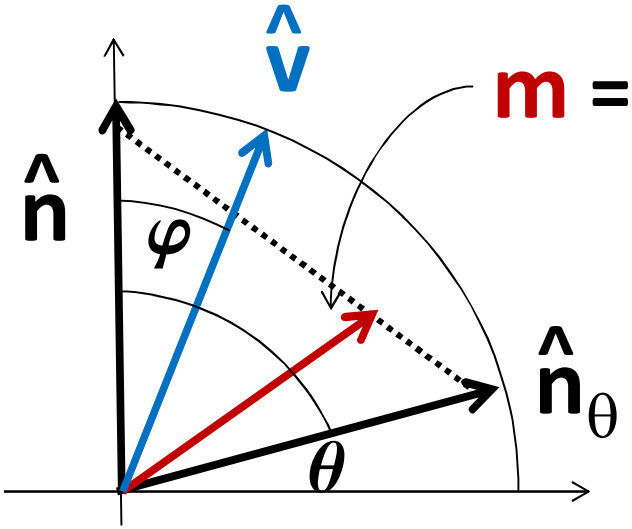
H. Massen, J. Uffink, Phys. Rev. Lett. 60, 1103, (1988)

Entropy H - unpredictability of measurement outcomes

The simplest uncertainty-like relation

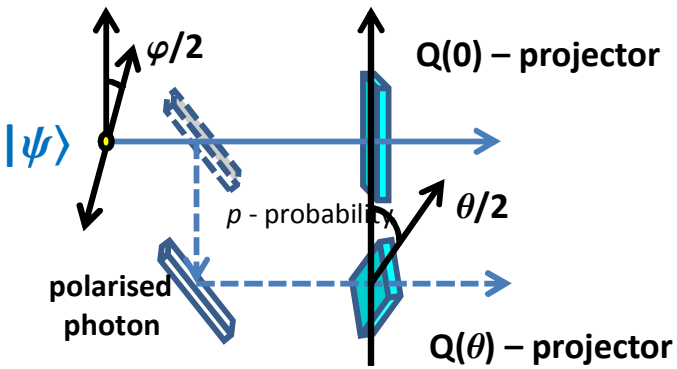


$$\Pr(\text{transmission}) := (1-p)\,\langle P(0)\rangle_{\psi} + p\,\langle P(\theta)\rangle_{\psi} \leq \xi(\theta,p) < 1$$



$$\mathbf{m} = (1-p)\,\mathbf{n} + p\,\mathbf{n}_\theta \qquad |\mathbf{m}| < 1$$

$$\xi(\theta,\mathrm{p}) = (1 + |\mathbf{m}|)/2$$



Pr (transmission) $\leq$ $\xi(\theta,\mathrm{p}) < 1$ is saturated

for „the most certain" v paralel to m

The Uncertainty Principle Determines the Nonlocality of Quantum Mechanics

Jonathan Oppenheim[1]* and Stephanie Wehner[2,3]*

Two central concepts of quantum mechanics are Heisenberg's uncertainty principle and a subtle form of nonlocality that Einstein famously called "spooky action at a distance." These two fundamental features have thus far been distinct concepts. We show that they are inextricably and quantitatively linked: Quantum mechanics cannot be more nonlocal with measurements that respect the uncertainty principle. In fact, the link between uncertainty and nonlocality holds for all physical theories. More specifically, the degree of nonlocality of any theory is determined by two factors: the strength of the uncertainty principle and the strength of a property called "steering," which determines which states can be prepared at one location given a measurement at another.

σ (*8*). Instead, $c_{T,\mathcal{D}}$ depends only on the measurements and hence quantifies their inherent incompatibility. It has been shown that for two measurements, entropic uncertainty relations do in fact imply Heisenberg's uncertainty relation (*9*), providing us with a more general way of capturing uncertainty [see (*10*) for a survey].

One may consider many entropic measures instead of the Shannon entropy. For example, the min-entropy

$$H_\infty(t)_\sigma := -\log \max_{x^{(t)}} p(x^{(t)}|t)_\sigma \qquad (4)$$

used in (*8*) plays an important role in cryptography and provides a lower bound on $H(t)_\sigma$. Entropic functions are, however, a rather coarse way of measuring the uncertainty of a set of measurements, as they do not distinguish the uncertainty inherent in obtaining any combination of outcomes $x^{(t)}$ for different measurements t. It is thus useful

[Science 330, 1072 (2010)]

CHSH inequality via quantum steering

$$\mathcal{P}_{win} = \Sigma_{a,x}\, p(x)\, p(a|x)\ \ \Sigma_y\, p(y)\, p(b = x.y \ominus a|a,x,y)\ \sigma_{a|x}$$

p(x)=p(y)=1/2
(free game)

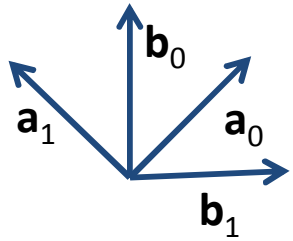
Bell game-type operator

$$\mathbf{B'} = \underbrace{\tfrac{1}{2} P_{+\mathbf{a}_0} \otimes \left(\tfrac{1}{2} P_{+\mathbf{b}_0} + \tfrac{1}{2} P_{+\mathbf{b}_1}\right)}_{(a,x)=(0,0)} + \underbrace{\tfrac{1}{2} P_{-\mathbf{a}_0} \otimes \left(\tfrac{1}{2} P_{-\mathbf{b}_0} + \tfrac{1}{2} P_{-\mathbf{b}_1}\right)}_{(a,x)=(1,0)} +$$

$$\underbrace{\tfrac{1}{2} P_{+\mathbf{a}_1} \otimes \left(\tfrac{1}{2} P_{+\mathbf{b}_0} + \tfrac{1}{2} P_{-\mathbf{b}_1}\right)}_{(a,x)=(0,1)} + \underbrace{\tfrac{1}{2} P_{-\mathbf{a}_1} \otimes \left(\tfrac{1}{2} P_{-\mathbf{b}_0} + \tfrac{1}{2} P_{+\mathbf{b}_1}\right)}_{(a,x)=(1,1)}$$

Optimal state $|\psi^+\rangle = (|V\rangle|V\rangle + |H\rangle|H\rangle)/\sqrt{2}$

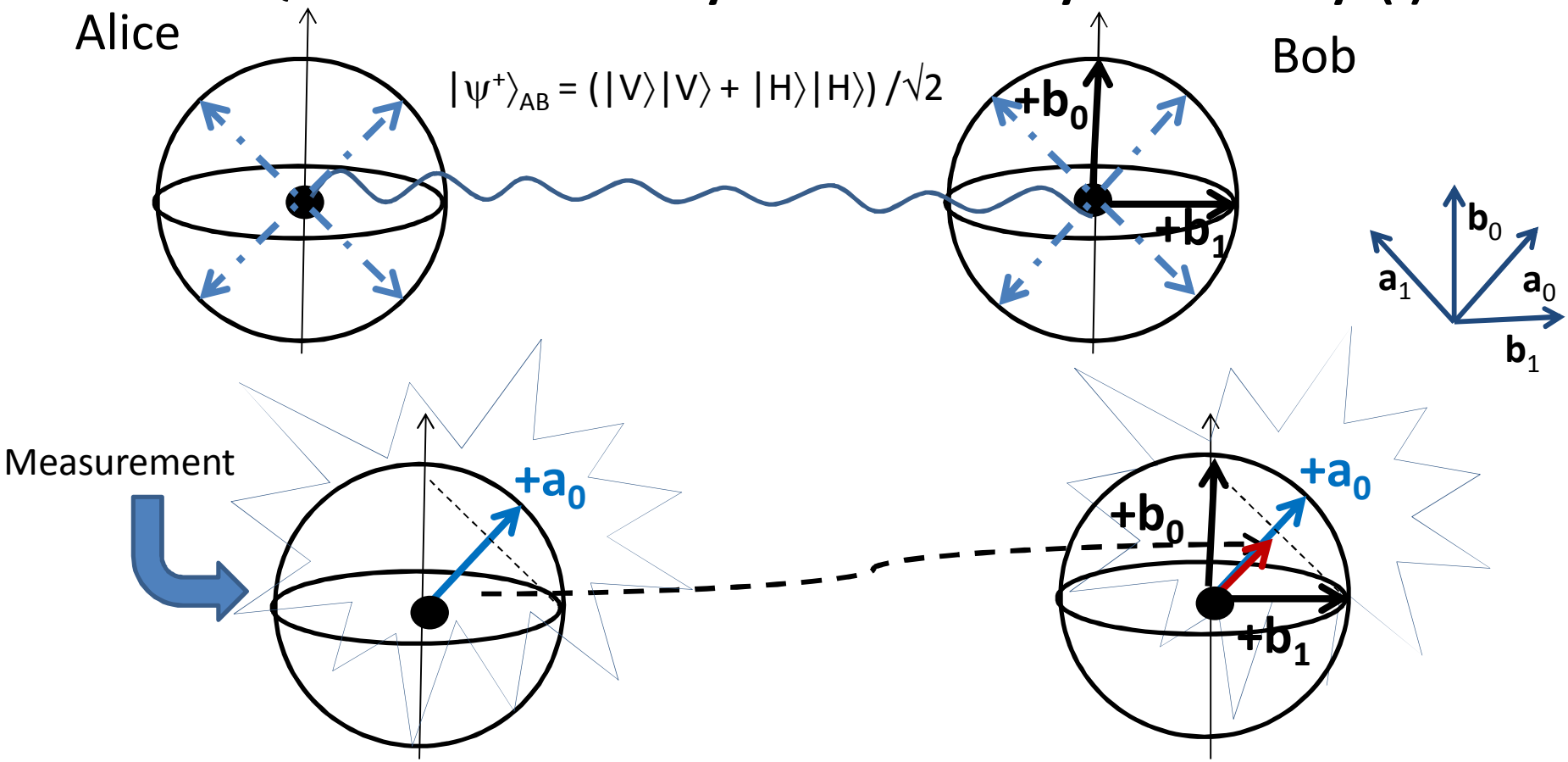
Optimal settings:



Quantum bound saturation

$$\mathcal{P}_{win} = \langle \mathbf{P'} \rangle_{\psi^+} = \langle \psi^+ | \mathbf{P'} | \psi^+ \rangle = \tfrac{1}{2} + \tfrac{1}{2}\, 2^{-1/2} = \mathbf{C_{QM}} < \mathbf{C_{NS}} = 1$$

Quantum nonlocality determined by uncertainty (I)



[J. Oppenheim, S. Wehner, Science (2010)]

$$\mathbf{B'} = \tfrac{1}{2} P_{+a_0} \otimes (\tfrac{1}{2} P_{+b_0} + \tfrac{1}{2} P_{+b_1}) + \tfrac{1}{2} P_{-a_0} \otimes (\tfrac{1}{2} P_{-b_0} + \tfrac{1}{2} P_{-b_1}) + \tfrac{1}{2} P_{+a_1} \otimes (\tfrac{1}{2} P_{+b_0} + \tfrac{1}{2} P_{-b_1}) + \tfrac{1}{2} P_{-a_1} \otimes (\tfrac{1}{2} P_{-b_0} + \tfrac{1}{2} P_{+b_1})$$

In any of the four Alice results she steers to the least uncertain quantum state !

True for any XOR game (ie involving the function $\chi(a,b|x,y) = 1 \Leftrightarrow a \oplus b = f(x,y)$

Quantum nonlocality determined by uncertainty (II)

[J. Oppenheim, S. Wehner, Science (2010)]

In general: $\mathcal{B}_{win} \leq \Sigma_{a,x}\, p(x)\, p(a|x)\, \xi^{(a,x)}$

Theorem. For any XOR game $\mathcal{B}_{win}$ saturated by Bob's uncertainty bounds.

$$\mathcal{B}_{win} = \Sigma_{a,x}\, p(x)\, p(a|x)\, \xi^{(a,x)} \quad \textbf{(!)}$$

Optimal state: **maximally entangled**

Optimal mesurements: **all Alice settings steer to „the most certain" state on Bob side.**

Question: Is it true for other quantum games / Bell inequalities ?

1) **Usually very hard to find optimal quantum value and optimal quantum state**
2) **To disprove one should show that the value is not saturated for any dimension of Hilbert space (!)**

New Bell game-type inequalities not saturating uncertainty principle

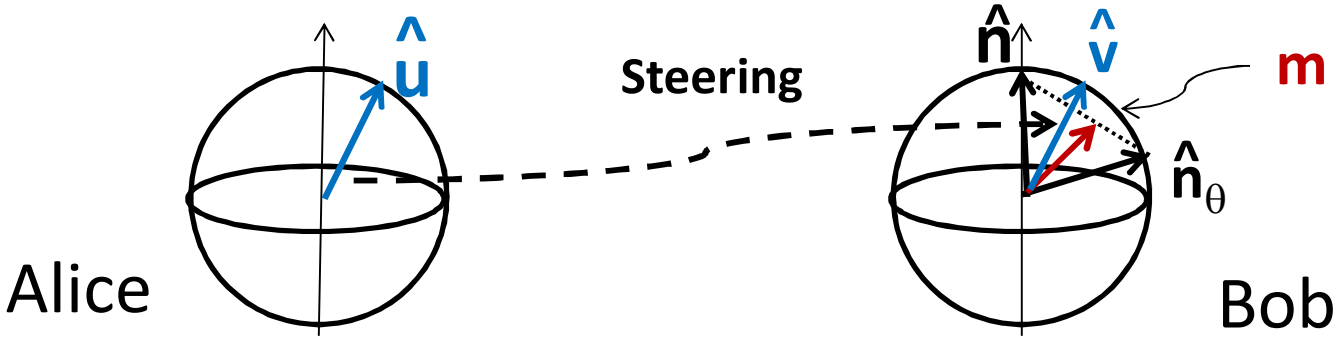
[R. Ramanathan, D. Goyeneche, P. Mironowicz, P. H. (2015)]

$$\mathcal{P}_{\mathbf{win}} \leq \mathbf{C_{QM}} < \Sigma_{a,x}\, p(x)\, p(a|x)\, \xi^{(a,x))}(\{p(y)\}, \chi) \quad (!)$$

global maxima, $\mathbf{C_{QM}}$ =0.545 (0.7822)
for the first (second) game

Remark. Only in the second inequality there is ,,true'' (two settings) uncertainty relation that is not saturated. In the firts there is the one-setting ,,uncertainty relation'' that Alice must not steer to if the winning probabilit is to be maximised.

Conclusion (main result). – Uncertainty relations do not determine optimal Bell value in game –type inequalities i.e. steering is not forced to ,,serve'' uncertainty by always creating remotely the ,,most certain'' state.
Shortly speaking the situation below is allowed while optimising Bell game - type inequality:



Towards equivalence of (probabilistic) quantum CC reduction and quantum nonlocality

$\mathbf{x} = [x_1,\ldots,x_n]$, $x_i \in \{0,1\}$ $\qquad$ $\mathbf{y} = [y_1,\ldots,y_n]$, $y_i \in \{0,1\}$

$\downarrow \qquad\qquad\qquad\qquad \downarrow$

Alice $\xleftrightarrow[\text{(classical or quantum) exchanged}]{\text{k information units}}$ Bob $\longrightarrow$ $f(\mathbf{x},\mathbf{y}) = ?$

C(f,p) – classical CC - minimal k of **bits** needed to compute $f(\mathbf{x},\mathbf{y})$ probabilistically with bounded bias

Q(f,p) – quantum CC - minimal k of **qubits** needed to compute $f(\mathbf{x},\mathbf{y})$ probabilistically with bounded bias

Probability of success
with bounded bias: $p \geq ½ + \varepsilon$, ε - independent on n

Extra assumption – inputs are randomised according to some $\mu(\mathbf{x},\mathbf{y})$.

Bounded bias - justification and pumping argument

Consider any protocol (classical or quantum) with

- communication complexity $\mathbf{C(f,p_S)}$
- the probability of success $\mathbf{p_S = ½ + \varepsilon}$, $\mathbf{½ < p_S < 2/3}$

Apply the protocol m times and **take majority** of outputs as a function f(**x**,**y**) value.

Remark. *Perfect analogy with biased coin when one does not know whether the bias is towards heads or tails. Resolution: toss it many times and claim that what is more frequent has a bias. The probability of right answer goes exponentially with a number of coin tosses.*

$$\boxed{p_S' \geq 1 - [\exp(-\varepsilon^2/2)]^m \xrightarrow{m \to \infty} 1}$$

Fast (exponential) amplification
(follows from so called Chernoff bound)

To get $p_S' \geq 2/3$ we need $m \geq 3/\varepsilon^2$ (♦)

and we must exchange not less than C(f,2/3) bits, so

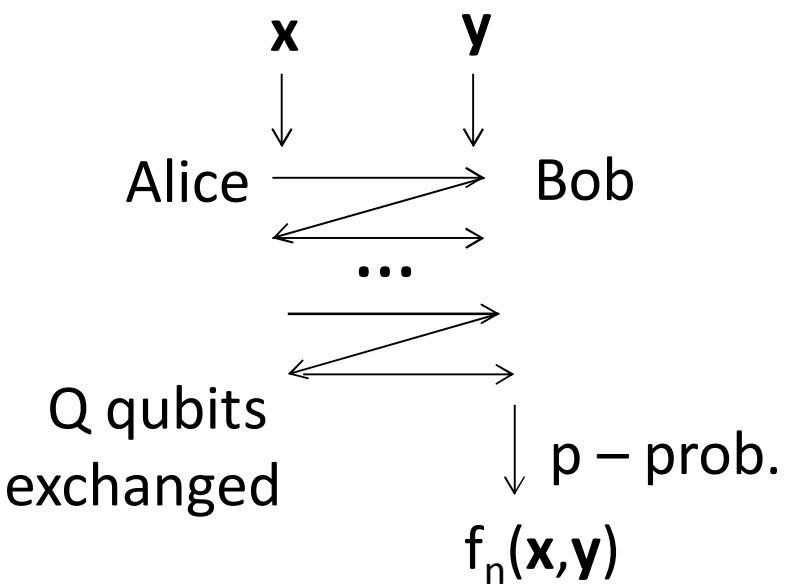
$$m\, C(f, p_S) \geq C(f,2/3) \overset{(♦)}{\Rightarrow} \boxed{C(f, p_S) \geq (p_S - ½)^2/3\, C(f,2/3)}$$

Transforming communication complexity advantage into quantum nonlocality

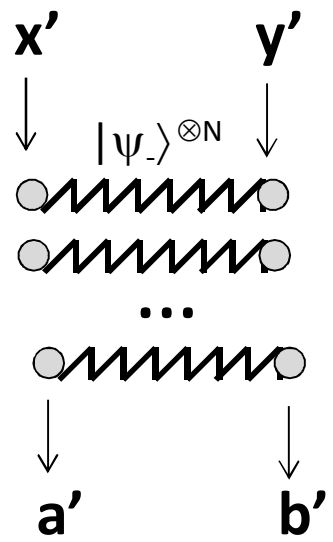
In literature quantum protocol with CC advantage were translated into entanglement Bell violation and vice versa. However in any case ***problem-specific analysis was needed*** *(e.g. specific technique, symmetry etc).*

Problem. Consider **arbitrary** Q qubits exchangins protocol with CC advantage over C(f,p) in calculation f(**x**,**y**).

Does any entanglement-based protocol with Bell inequality violation exist that is linked to it ?



?



$Q \ll C(f_n,p)$

(ie. $Q/C(f_n,p) \to 0$ for large n)

$B_Q \gg B_{LHV}$

(with degree of violation depending on Q, $C(f_n,p)$)

General form of quantum protocol reducing CC

0. Initially product state $|\Psi\rangle_{A_0} |\Psi\rangle_{B_0}$

1. Alice performs isometry $U_{\mathbf{x}}^{A_0 \to A_1 M_1}$ and sends M_1

2. Bob performs isometry $U_{\mathbf{y}}^{B_0 M_1 \to B_1 M_2}$ and sends M_2 back

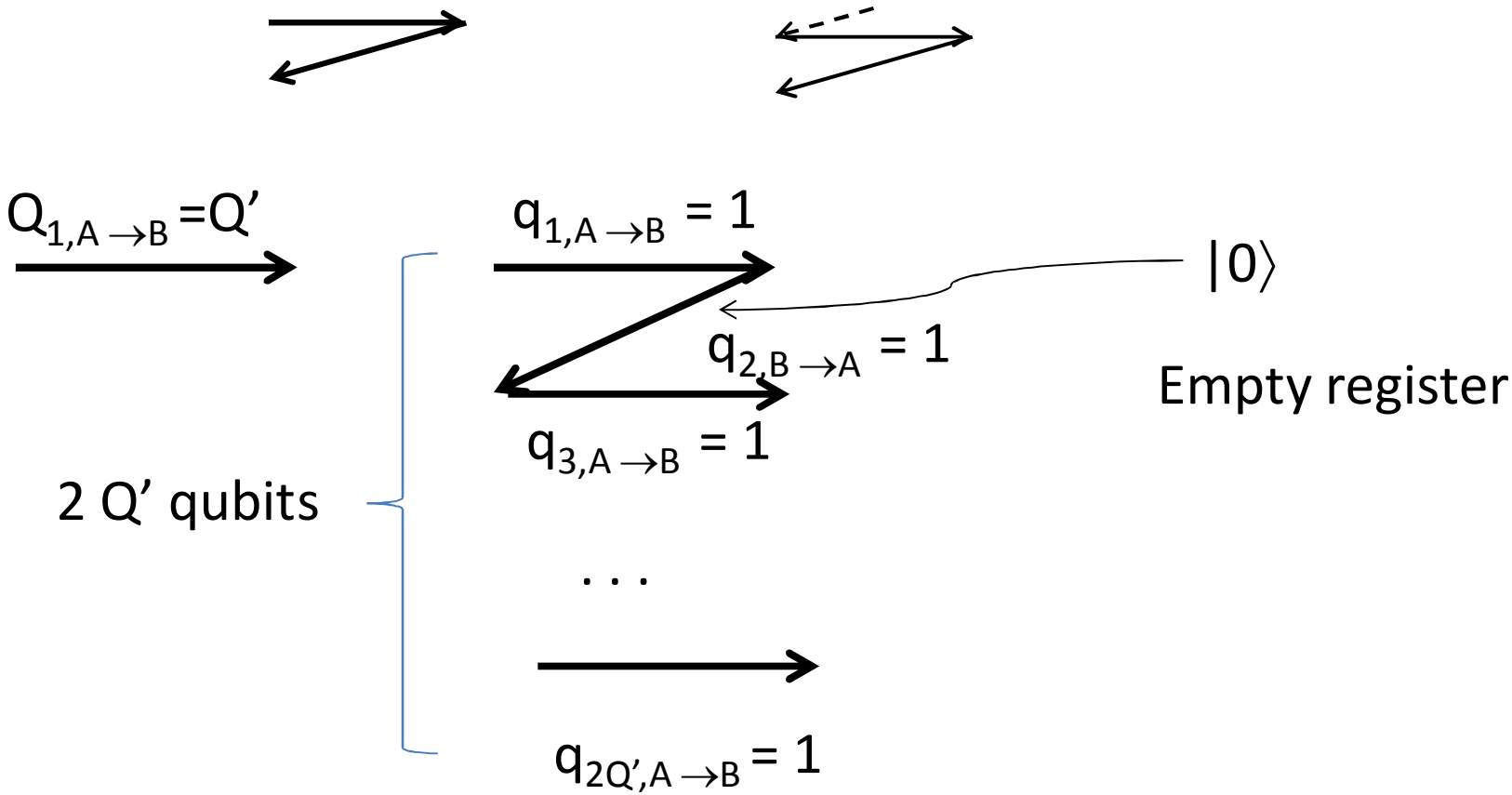
3. The parties repeat it r - 1 rouds.
In the last roud instead isometry Bob performs
the measurement and outputs the value of f(**x**,**y**)

Quantum messages M_i are considered to be multiqubit (Q_i) messages. Total amount of quantum qubits exchanged

$$Q = \Sigma_i Q_i \ .$$

Technical reductions – qubit rounds

$$Q = (Q_{1,A\to B} + Q_{1,B\to A}) + (Q_{2,A\to B} + Q_{2,B\to A}) + \ldots$$



Q protocol translated into 2Q protocol
with 1 qubit exchanged in each round.

We will consider qubit protocol form now, dropping the factor 2.

Technical reductions – limiting the memory (I)

0. Initially product state $|\Psi\rangle_{A_0} \; |\Phi\rangle_{B_0}$

1. Alice performs isometry $U_{\mathbf{x}}^{A_0 \to A_1 M_1}$ and sends **qubit** M_1

2. Bob performs isometry $U_{\mathbf{y}}^{B_0 M_1 \to B_1 M_2}$ and sends M_2 **qubit** back.

$$\Big(|\Psi\rangle |0\rangle \Big) |\Phi\rangle \xrightarrow{\text{isometry}} \Big(|\Psi_0\rangle |0\rangle + |\Psi_1\rangle |1\rangle \Big) |\Phi\rangle \xrightarrow{\text{sending}}$$

$$|\Psi_0\rangle \Big(|0\rangle |\Phi\rangle \Big) + |\Psi_1\rangle \Big(|1\rangle |\Phi\rangle \Big) \xrightarrow{\text{isometry}}$$

$$|\Psi_0\rangle \Big(|0\rangle |\Phi_{00}\rangle + |1\rangle |\Phi_{01}\rangle \Big) + |\Psi_1\rangle \Big(|1\rangle |\Phi_{10}\rangle + |1\rangle |\Phi_{11}\rangle \Big) \xrightarrow{\text{sending}}$$

$$\Big(|\Psi_0\rangle |0\rangle \Big) |\Phi_{00}\rangle + \Big(|\Psi_0\rangle |1\rangle \Big) |\Phi_{01}\rangle + \Big(|\Psi_1\rangle |1\rangle \Big) |\Phi_{10}\rangle + \Big(|\Psi_1\rangle |1\rangle \Big) |\Phi_{11}\rangle \Big)$$

...

Technical reductions – bounding the memory size

$$\left(|\Psi_0\rangle|0\rangle\right)|\Phi_{00}\rangle + \left(|\Psi_0\rangle|1\rangle\right)|\Phi_{01}\rangle + \left(|\Psi_1\rangle|1\rangle\right)|\Phi_{10}\rangle + \left(|\Psi_1\rangle|1\rangle\right)|\Phi_{11}\rangle\Big)$$

Fact. After r rounds the total quantum state is of the form

$$\Sigma_{\mathbf{x}\in\{0,1\}^r}|\Psi_{\mathbf{x}}\rangle\left(|x_r\rangle\ |\Phi_{\mathbf{x}}\rangle\right) \qquad \mathbf{x} = [x_1,\ldots,x_r]$$

Only 2^r different vectors (either $|\Psi_{\mathbf{x}}\rangle$ or $|\Phi_{\mathbf{x}}\rangle$) on each side, hence they represent

$$\log 2^r = r = \mathbf{Q}$$

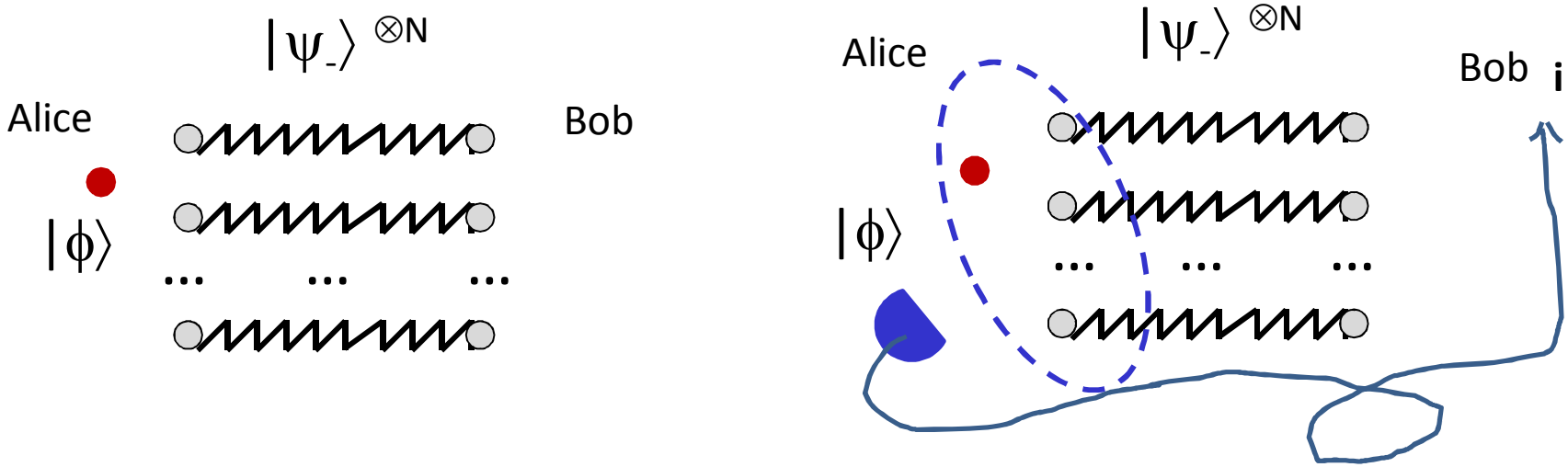
memory (since in each round single qubit sent and Q is the total no. of qubit messages).

Total memory 2Q +1

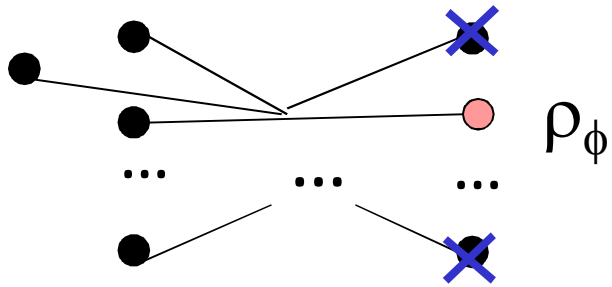
Towards universal linking CC to quantum nonlocality
Port-based teleportation

Max. entangled state

$|\psi_-\rangle$



Measurement result **i** $\in$ **{1, …, N}**



ρ_ϕ **(i-th position)**

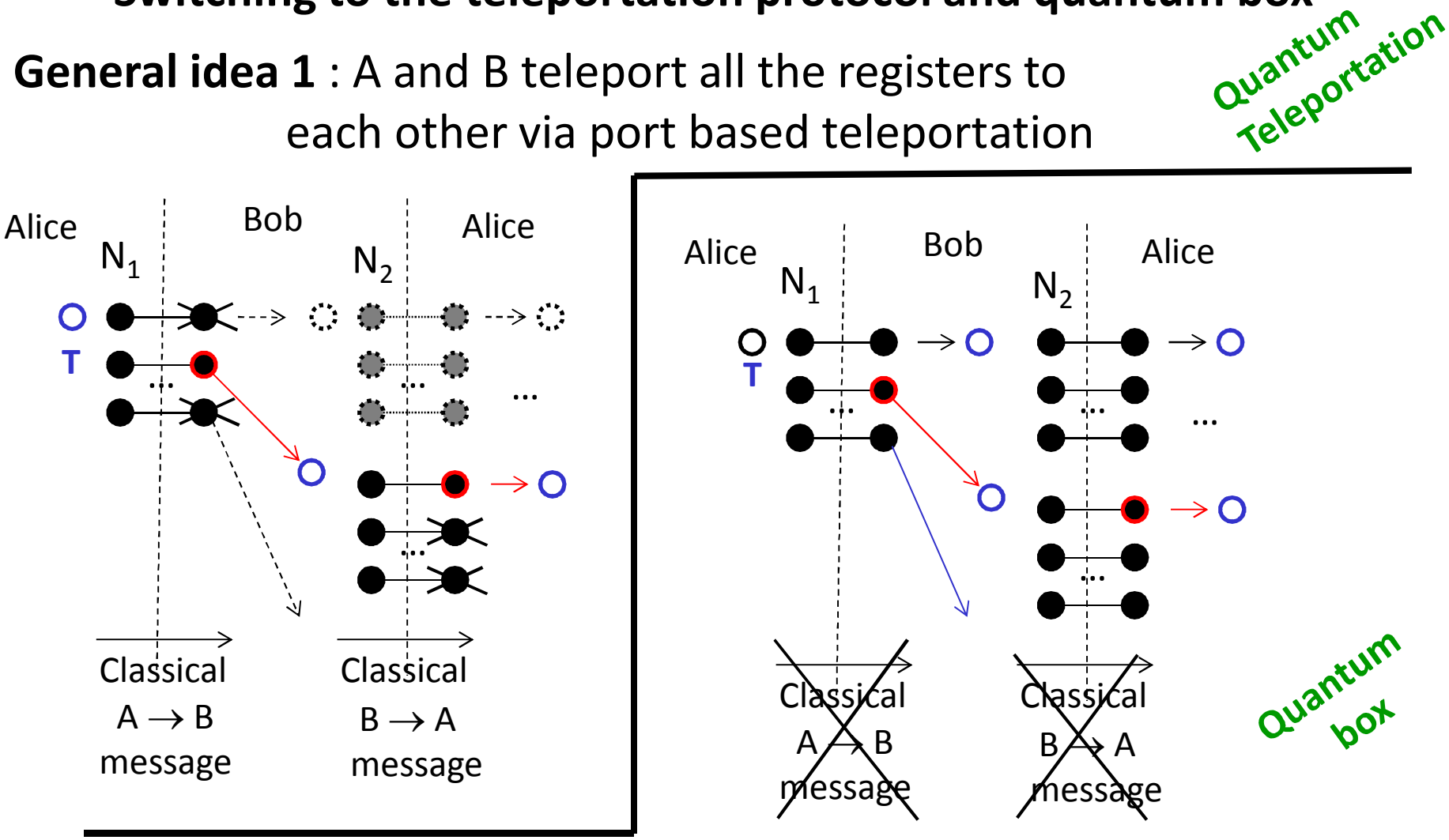
[S. Ishizaka, T. Hiroshima,
Phys. Rev. Lett. (2008),
E. Knill, R. Laflamme, G. J. Milburn
Nature (2001)]

Transmission fidelity

$$f_{\text{transmission}} := \langle\phi|\rho_\phi|\phi\rangle \geq 1 - d^2/N \xrightarrow{N \to \infty} 1$$

Switching to the teleportation protocol and quantum box

General idea 1 : A and B teleport all the registers to each other via port based teleportation



General idea 2 : A and B ,,pretend'' teleportation of any register in their hands, but keep the results of measurements and do not send them. Exponentially more active systems.

State fidelity and success probability in teleportation

Previous final state ρ Success probability $p_S = \mathrm{Tr}(M_S\,\rho)$, $0 \le M_S \le I$

New final state ρ^{tel} New success probability $p^{tel}_S = \mathrm{Tr}(M_S\,\rho^{tel})$

$$p_S - p^{tel}_S \le \mathrm{Tr}(M_S(\rho' - \rho)) \le \mathrm{Tr}|\rho' - \rho| \overset{(\blacklozenge)}{\le} 2(1 - F^2(\rho^{tel},\rho))^{-1/2}$$

$$p_S = \tfrac{1}{2} + \varepsilon, \quad F(\rho^{tel},\rho) = F^{2r} = F^{2Q}$$

(qubit protocol, success in all 2r rounds)

In one round of the teleportation $(1 \le i \le 2r)$

$d = 2^{2Q+1}$ (both memories teleported),

$N_i = 2^{5Q}$ (choice of no. of ports, $\log N_i = 5Q$ bits of comm.)

$$F \ge 1 - (d^2 / N_i) \ge 1 - 2^{-Q+2}$$

Bits communicated $\mathbf{C_q} = \sum_{i=1}^{2r-1} \log N_i \le 2r\,5Q = \mathbf{10\,Q^2}$

$$\mathbf{p^{tel}_S \ge \tfrac{1}{2} + \varepsilon - 2[1 - (1 - 2^{-Q+2})^{2Q}]^{-1/2}} \xrightarrow{Q \to \infty} \mathbf{p_S}$$

(♦) [C. A. Fuchs, J. van de Graaf, arXiv:quant-ph/9712042, *IEEE* Transactions on IT (1999)]

Summary and step towards quantum nonlocality (I)

Quantum CC reduction protocol

$\rightleftarrows$ Q qubits

+

$\approx$ 2Q memory

$B_{QCC} = p_S - ½ = \varepsilon$ (bias independent on n)

Quantum teleportation based protocol

Singlets + local measurements

$\rightleftarrows$ $C = 10\,Q^2$ bits

$B^{tel} = \varepsilon - 2[1 - (1 - 2^{-Q+2})^{2Q}]^{-½} \approx B_{QCC}$

Quantum box

Singlets + local measurements

No communication

$$B^{box} = \Sigma_{\mathbf{x}\,\mathbf{y}}\ \mu(\mathbf{x},\mathbf{y})\ \Sigma_{(ab)\in\mathcal{P}}\, p(o_q = f(\mathbf{x},\mathbf{y})\,|\,\mathbf{xy})$$

Explanation. $\mathcal{P}$ – all alternative teleportation paths.
Remark. x', y' are measurement settings, they depend on **x**,**y** , but have different character (ie. are directly associated with the teleportation POVMs)

$$B^{box} = \varepsilon - 2[1 - (1 - 2^{-Q+2})^{2Q}]^{-½} \approx B_{QCC}$$

Towards Bell inequality candidate

Quantum box B_Q

Singlets + local measurements No communication

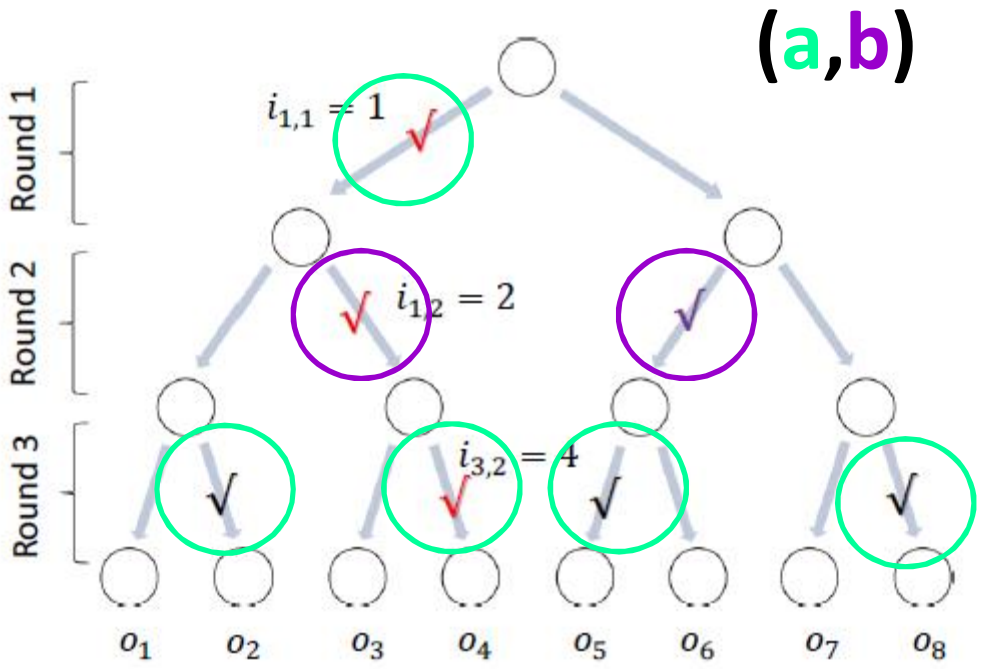
$$B^{box} = [\ \Sigma_{\mathbf{x}\,\mathbf{y}}\ \mu(\mathbf{x},\mathbf{y})\ \Sigma_{(ab)\,:\,g(a,b)\in\mathcal{P}}\, p(o_q = f(\mathbf{x},\mathbf{y}) \mid \mathbf{xy})\ ] - \tfrac{1}{2}$$

Explanation. $\mathcal{P}$ – all alternative teleportation paths.
Remark. x', y' are measurement settings,
they depend on **x**,**y** , but have different character
(ie. are directly associated with the teleportation POVMs)

$$B(B_Q) = \varepsilon - \mathbf{2[1-(1-2^{-Q+2})^{2Q}]^{-\frac{1}{2}}} \approx B_{QCC}$$

(a,b) – result of the measurements on the quantum box

$\mathcal{P}$ = {g(ab) – paths from the top to the bottom: √ √ √)



Deriving Bell inequality for CC problems

Class of problems: communication complexity problem with randomised input (**x**,**y**).
Requirement: probability of success with bounded bias for all outputs.
Shared randomness does not help, here so LHV boxes (classical boxes) do not help.

$C(f, p_S)$ – classical (optimal) CC of some function $C(f, p_S)$ for randomised protocol. The same if assisted **with any shared classical box P_{LHV}**. It will also obey ,,pumping'' restriction.

$$C(f, p_S) \geq (p_S - ½)^2/3\, C(f,2/3) \qquad 0 < p_S < 2/3$$

$$C \geq (p_S - ½)^2/3\, C(f,2/3)$$

$C \geq C(f, p_S)$ for any C needed to achieve p_S.

$$\boxed{B(P_{LHV}) = p_S(P_{LHV}) - ½ \leq [\, 3C / C(f,2/3)\,]^{-½}}$$

$$B = B^{box} = [\ \Sigma_{\mathbf{x}\,\mathbf{y}}\ \mu(\mathbf{x},\mathbf{y})\ \Sigma_{(ab)\,:\,g(a,b)\in \mathcal{P}}\, p(o_q = f(\mathbf{x},\mathbf{y}) \mid \mathbf{xy})\ ] - ½$$

Alice and Bob sends each other (in a sequence) all the information C needed to retrieve o_q at Bob site. Bob to get the result.
This is a specific protocol of getting the bias $B(P_{LHV})$.

Classical - quantum separation

$$B(P_{LHV}) = p_S(P_{LHV}) - \tfrac{1}{2} \leq [\, 3C / C(f,2/3)\,]^{-1/2}$$

The box has the same input-output structure as the quantum one, and the success probability is calculated in the same way.

Take now $C = 10\, Q^2$

$$B(P_Q) = \varepsilon - 2[1 - (1 - 2^{-Q+2})^{2Q}]^{-1/2} \approx B_{QCC}\,, \quad \text{usually } \varepsilon = 1/6$$

$$\boxed{\frac{B(P_Q)}{B(P_{LHV})} \geq \frac{\sqrt{C(f,2/3)}}{Q\sqrt{30}}\,[\,1/6 - 2\,[1 - (1 - 2^{-Q+2})^{2Q}]^{-1/2}\,]}$$

,,Vector in subspace Problem''

$$\begin{cases} p^Q_S \geq \tfrac{1}{2} - (1-2^{-\log n})^2 \\ p^{cl}_S \leq \tfrac{1}{2} + [10 \log^2 n / \sqrt[4]{n}\,] \end{cases} \Rightarrow \frac{B(B_Q)}{B(B_{LHV})} \geq \Omega(\sqrt[4]{n}/\log n)$$

Summary

- Sophisticated LHV caused by faster-than-light speed impossible : would remove nosignaling (NS)
- Monogamy – important form the perspecitve of security tasks.
- Can be made more tight, by careful examining contradictions with local realism.
- Geometry of quantum correlations within NS nontrivial.
- Implies impossibility of application of monogamy against NS adversary. some tasks harder because of that.
- Practical way of testing quantumness of correlations: semidefinite programming.
- Physical principles to restore quantum correlations – some of them intuitively natural and fundamental (like IC)
- Interesting steering and uncertainty link. Sometimes optimal Bell inequality violation forces Alice to steer to the most certain state at Bob site.
- For broad class of protocols it is possible to convert quantum communication complexity advantage in the well defined sense into some Bell inequality. The latter is violated whenever $Q^2 << C$.

Thank you

Krajowe Centrum Informatyki Kwantowej

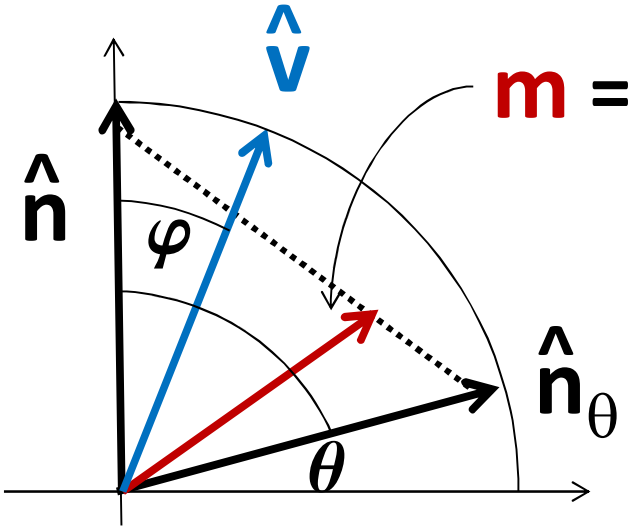
National Quantum Information Centre of Gdańsk (NQuantIC)

ul. Wł. Andersa 27
81-824 Sopot

http://www.kcik.univ.gda.pl/

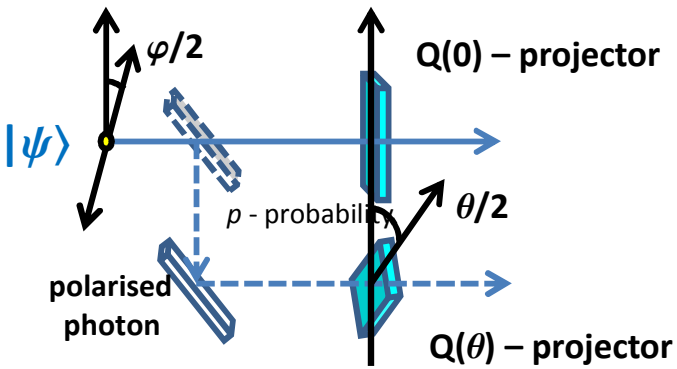
Plan

- LHV, quantum and no-signaling correlations
- Quantum correlations and the issue of faster than light communication
- Describing Q by SDP hierarchy
- Geometry of Q versus NS and consequences
- Monogamy of NS correlations
- Communication complexity - a simple example
- Physical principles aiming at restoring Q
- Violation of Bell inequality and uncertanity relations
- Deriving Bell inequality problem form quantum communication complexity advantage.



$$\mathbf{m} = (1-p)\,\mathbf{n} + p\,\mathbf{n}_\theta \qquad |\mathbf{m}| < 1$$

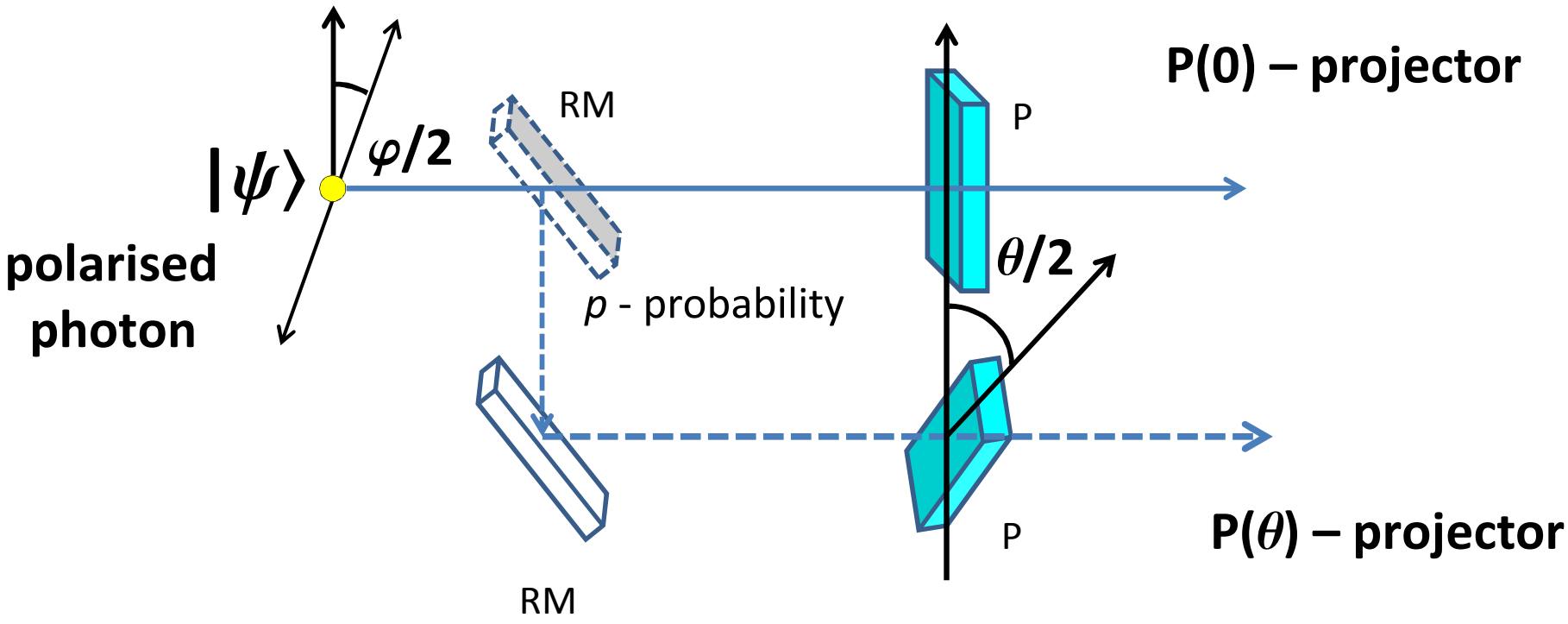
$$\xi(\theta,\mathrm{p}) = (1 + |\mathbf{m}|)/2$$



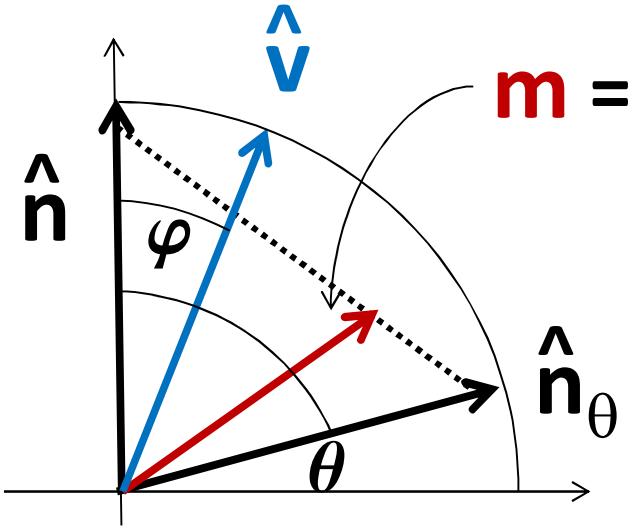
Pr (transmission) $\leq$ $\xi(\theta,\mathrm{p}) < 1$ is saturated

for „the least uncertain" v paralel to m

The simplest uncertainty-like relation

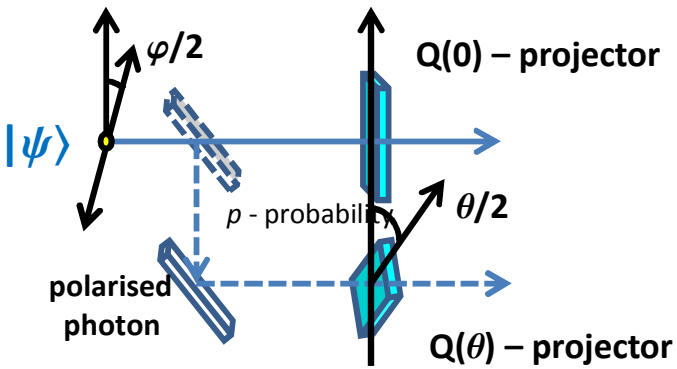


$$\Pr(\text{transmission}) := (1-p)\,\langle P(0)\rangle_{\psi} + p\,\langle P(\theta)\rangle_{\psi} \leq \xi(\theta,p) < 1$$



$$\mathbf{m} = (1-p)\,\mathbf{n} + p\,\mathbf{n}_\theta \qquad |\mathbf{m}| < 1$$

$$\xi(\theta,\mathrm{p}) = (1 + |\mathbf{m}|)/2$$



Pr (transmission) $\leq$ $\xi(\theta,\mathrm{p}) < 1$ is saturated

for „the least uncertain" v paralel to m

The Uncertainty Principle Determines the Nonlocality of Quantum Mechanics

Jonathan Oppenheim[1]* and Stephanie Wehner[2,3]*

Two central concepts of quantum mechanics are Heisenberg's uncertainty principle and a subtle form of nonlocality that Einstein famously called "spooky action at a distance." These two fundamental features have thus far been distinct concepts. We show that they are inextricably and quantitatively linked: Quantum mechanics cannot be more nonlocal with measurements that respect the uncertainty principle. In fact, the link between uncertainty and nonlocality holds for all physical theories. More specifically, the degree of nonlocality of any theory is determined by two factors: the strength of the uncertainty principle and the strength of a property called "steering," which determines which states can be prepared at one location given a measurement at another.

σ (*8*). Instead, $c_{T,\mathcal{D}}$ depends only on the measurements and hence quantifies their inherent incompatibility. It has been shown that for two measurements, entropic uncertainty relations do in fact imply Heisenberg's uncertainty relation (*9*), providing us with a more general way of capturing uncertainty [see (*10*) for a survey].

One may consider many entropic measures instead of the Shannon entropy. For example, the min-entropy

$$H_\infty(t)_\sigma := -\log \max_{x^{(t)}} p(x^{(t)}|t)_\sigma \qquad (4)$$

used in (*8*) plays an important role in cryptography and provides a lower bound on $H(t)_\sigma$. Entropic functions are, however, a rather coarse way of measuring the uncertainty of a set of measurements, as they do not distinguish the uncertainty inherent in obtaining any combination of outcomes $x^{(t)}$ for different measurements t. It is thus useful

[Science 330, 1072 (2010)]

CHSH inequality via quantum steering

$$\mathcal{P}_{win} = \Sigma_{a,x}\ p(x)\ p(a|x)\ \Sigma_y\, p(y)\ p(b = x.y \ominus a|a,x,y)\ \sigma_{a|x}$$

p(x)=p(y)=1/2
(free game)

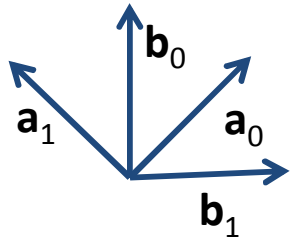
Bell game-type operator

$$\mathbf{P'} = \underbrace{\tfrac{1}{2} P_{+\mathbf{a}_0} \otimes (\tfrac{1}{2} P_{+\mathbf{b}_0} + \tfrac{1}{2} P_{+\mathbf{b}_1})}_{(a,x)=(0,0)} + \underbrace{\tfrac{1}{2} P_{-\mathbf{a}_0} \otimes (\tfrac{1}{2} P_{-\mathbf{b}_0} + \tfrac{1}{2} P_{-\mathbf{b}_1})}_{(a,x)=(1,0)} +$$

$$\underbrace{\tfrac{1}{2} P_{+\mathbf{a}_1} \otimes (\tfrac{1}{2} P_{+\mathbf{b}_0} + \tfrac{1}{2} P_{-\mathbf{b}_1})}_{(a,x)=(0,1)} + \underbrace{\tfrac{1}{2} P_{-\mathbf{a}_1} \otimes (\tfrac{1}{2} P_{-\mathbf{b}_0} + \tfrac{1}{2} P_{+\mathbf{b}_1})}_{(a,x)=(1,1)}$$

Optimal state $|\psi^+\rangle = (|V\rangle|V\rangle + |H\rangle|H\rangle)/\sqrt{2}$

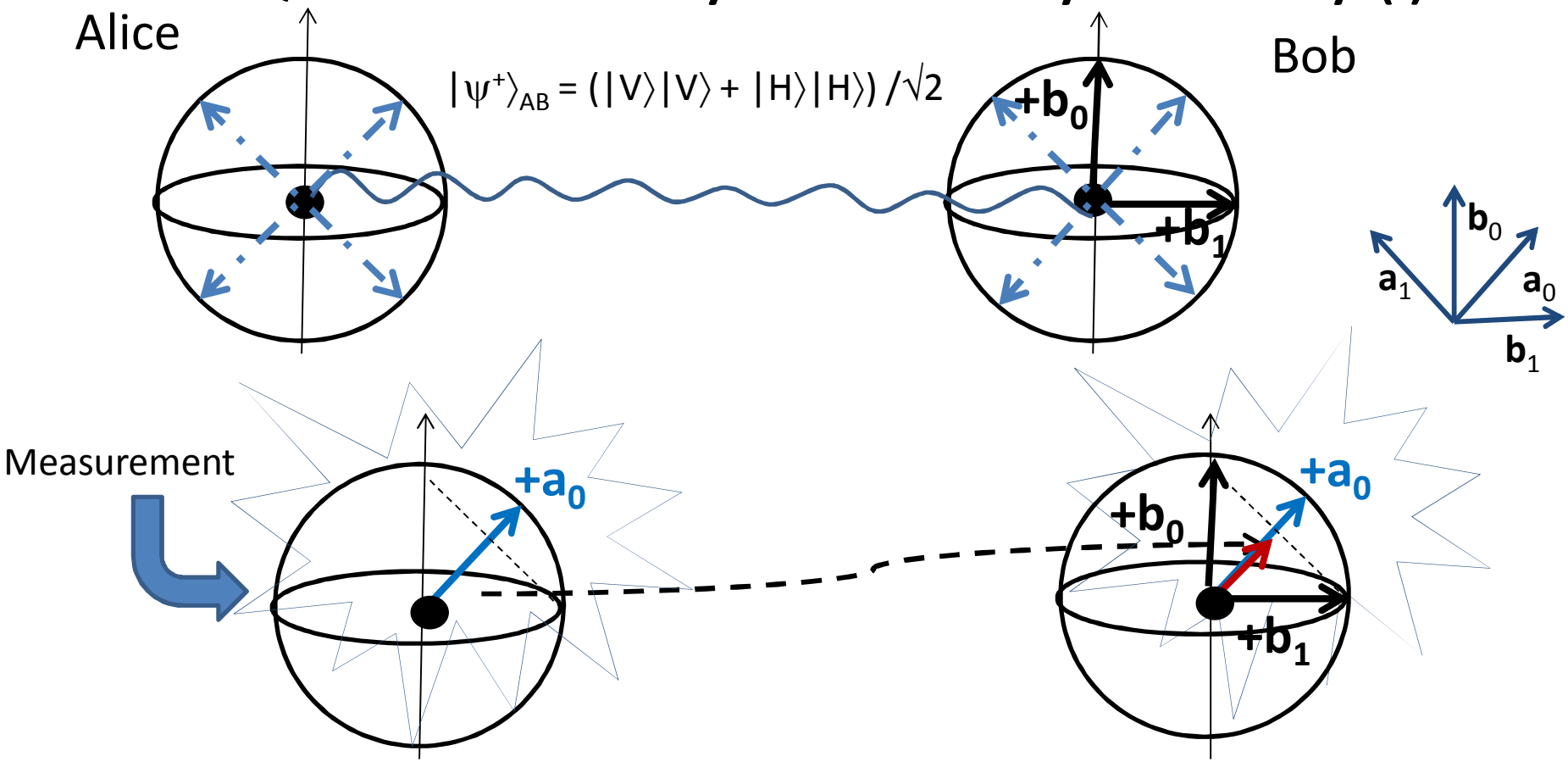
Optimal settings:



Quantum bound saturation

$$\mathcal{P}_{win} = \langle \mathbf{P'} \rangle_{\psi^+} = \langle \psi^+ | \mathbf{P'} | \psi^+ \rangle = \tfrac{1}{2} + \tfrac{1}{2}\, 2^{-1/2} = \mathbf{C_{QM}} < \mathbf{C_{NS}} = 1$$

Quantum nonlocality determined by uncertainty (I)



[J. Oppenheim, S. Wehner, Science (2010)]

$$\mathbf{P'} = \tfrac{1}{2} P_{+a_0} \otimes (\tfrac{1}{2} P_{+b_0} + \tfrac{1}{2} P_{+b_1}) + \tfrac{1}{2} P_{-a_0} \otimes (\tfrac{1}{2} P_{-b_0} + \tfrac{1}{2} P_{-b_1}) + \tfrac{1}{2} P_{+a_1} \otimes (\tfrac{1}{2} P_{+b_0} + \tfrac{1}{2} P_{-b_1}) + \tfrac{1}{2} P_{-a_1} \otimes (\tfrac{1}{2} P_{-b_0} + \tfrac{1}{2} P_{+b_1})$$

In any of the four Alice results she steers to the least uncertain quantum state !

True for any XOR game (ie involving the function $\chi(a,b|x,y) = 1 \Leftrightarrow a \oplus b = f(x,y)$

Quantum nonlocality determined by uncertainty (II)

[J. Oppenheim, S. Wehner, Science (2010)]

In general: $\mathcal{P}_{win} \leq \Sigma_{a,x}\, p(x)\, p(a|x)\, \xi^{(a,x)}$

Theorem. For any XOR game $\mathcal{P}_{win}$ saturated by Bob's uncertainty bounds.

$$\mathcal{P}_{win} = \Sigma_{a,x}\, p(x)\, p(a|x)\, \xi^{(a,x)} \quad \textbf{(!)}$$

Optimal state: **maximally entangled**

Optimal mesurements: **all Alice settings steer to „the least uncertain" state on Bob side.**

Question: Is it true for other quantum games / Bell inequalities ?

1) **Usually very hard to find optimal quantum value and optimal quantum state**
2) **To disprove one should show that the value is not saturated for any dimension of Hilbert space (!)**

New Bell game-type inequalities with analytical quantum bounds (II)

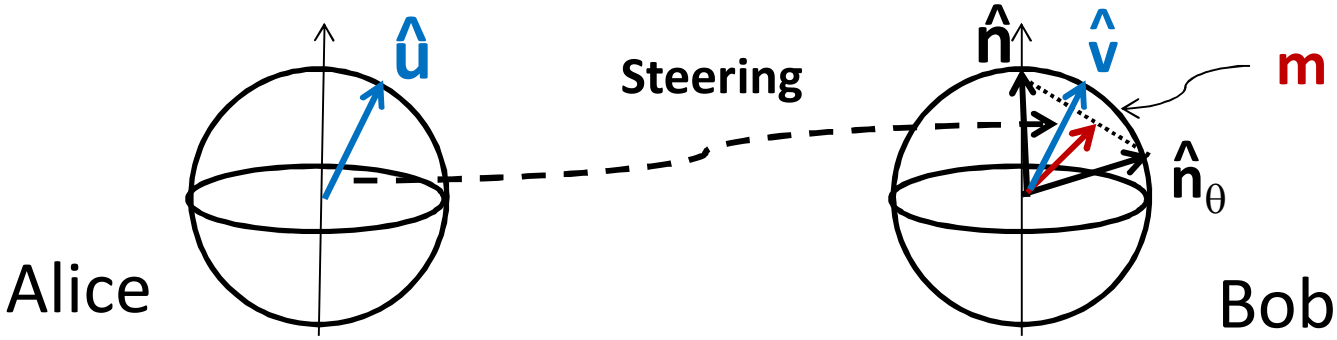
[R. Ramanathan, D. Goyeneche, P. Mironowicz, P. Horodecki (2015)]

$$\mathcal{P}_{\mathbf{win}} \leq \mathbf{C_{QM}} < \Sigma_{a,x}\, p(x)\, p(a|x)\, \xi^{(a,x))}(\{p(y)\}, \chi) \quad (!)$$

global maxima, $\mathbf{C_{QM}}$ =0.545 (0.7822)
for the first (second) game

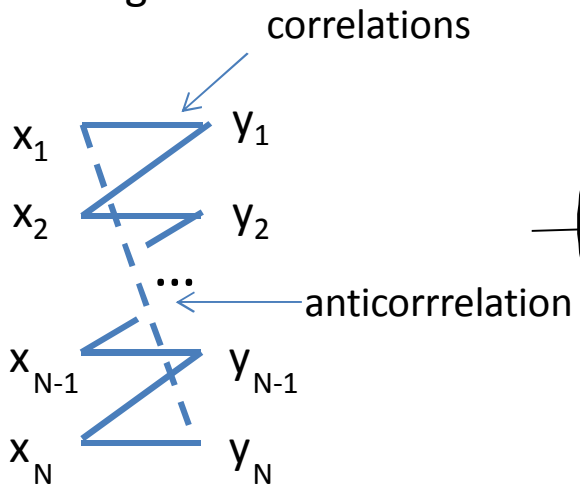
Remark. Only in the second inequality there is ,,true'' (two settings) uncertainty relation that is not saturated. In the firts there is the one-setting ,,uncertainty relation'' that Alice must not steer to if the winning probabilit is to be maximised.

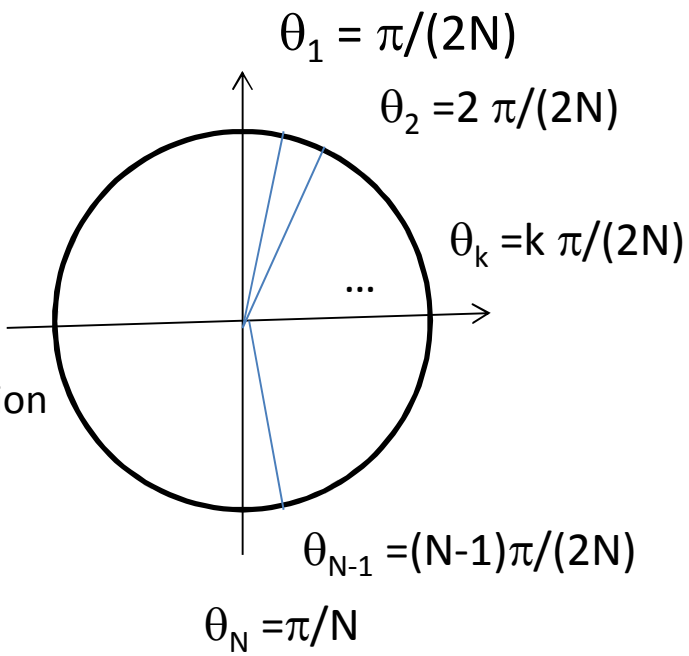
Conclusion (main result). – Uncertainty relations do not determine optimal Bell value in game –type inequalities i.e. steering is not forced to ,,serve'' uncertainty by always creating remotely the ,,least'' uncertaint state.
Shortly speaking the situation below is allowed while optimising Bell game - type inequality:



Chain inequality

Only the same or nest neighbours settings with perfect correlation. θ_N and θ_1 closintg the chain with antycorrelation.





Probabilities of winning:

$C_{LVH} = 1 - 1/2N$

$C_Q = 1 - \sin^2(\pi/4N)$

$C_{NS} = 1$

It is better to compare probabilities of ,,loosing the game'':

$\beta_{LVH} = 1/2N$

$\beta_Q = \sin^2(\pi/4N)$

$\beta_{NS} = 0$

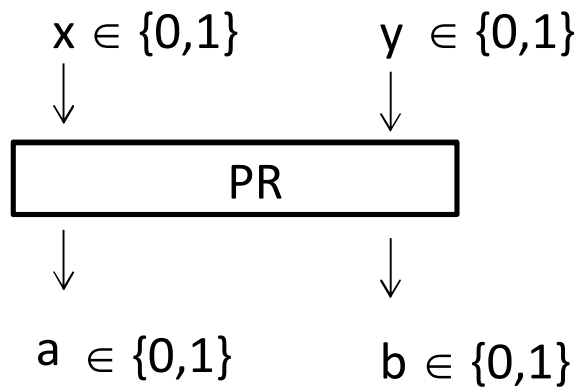
$$\beta_Q/\beta_{LVH} \xrightarrow{N\to\infty} 0$$

Quantum value approaches NS limit faster

PR box as an example of nosignaling correlations (I)

Popescu Rohlich box (1994). Binary inputs (”two settings”), binary outputs.

$$p(ab|xy) = \begin{cases} \frac{1}{2} & (a, b):\ a \oplus b = x\,y \\ 0 & \text{otherwise} \end{cases}$$



Remark. Notice that $a \oplus b = (a+b) \bmod 2$
so $a \oplus b = 0$ unless $x=y=1$ means
,,a = b unless x=y=1 when they are opposite’’.

Normalisation. $\Sigma_{ab} p(ab|xy)=1$ means:
,,sum = 1’’ for any square with fixed x,y.

No – signaling (NS). Why is it no-signaling ?

$\Sigma_b p(ab|xy) := p(a|xy) = p(a|x)$ means: in any **row** sums for the small rectangles are equal (**no y-dependence**)

$\Sigma_a p(ab|xy) := p(b|xy) = p(b|y)$ means: in any **column** sums for the small rectangles are equal (**no x – dependence**)

Table of conditional probablities.

	y	0		1	
x	a \ b	0	1	0	1
0	0	1/2		1/2	
	1		1/2		1/2
1	0	1/2			1/2
	1		1/2	1/2	

PR box as an example of nosignaling correlations (II)

p(ab|xy)

x	a \ b, y	0	1	0	1
0	0	1/2		1/2	
	1		1/2		1/2
1	0	1/2			1/2
	1		1/2	1/2	

$$\Sigma_b\, p(ab|xy) := p(a|xy) \overset{?}{=} p(a|x)$$

x	a \ y	0	1
0	0	1/2	1/2
	1	1/2	1/2
1	0	1/2	1/2
	1	1/2	1/2

p(a|x1)

p(a|x0)

Columns the same **:= p(a|x)**

Signaling box :

q(ab|xy)

x	a \ b, y	0	1	0	1
0	0	1/2		1/3	1/3
	1		1/2		1/3
1	0	1/2			1/2
	1		1/2	1/2	

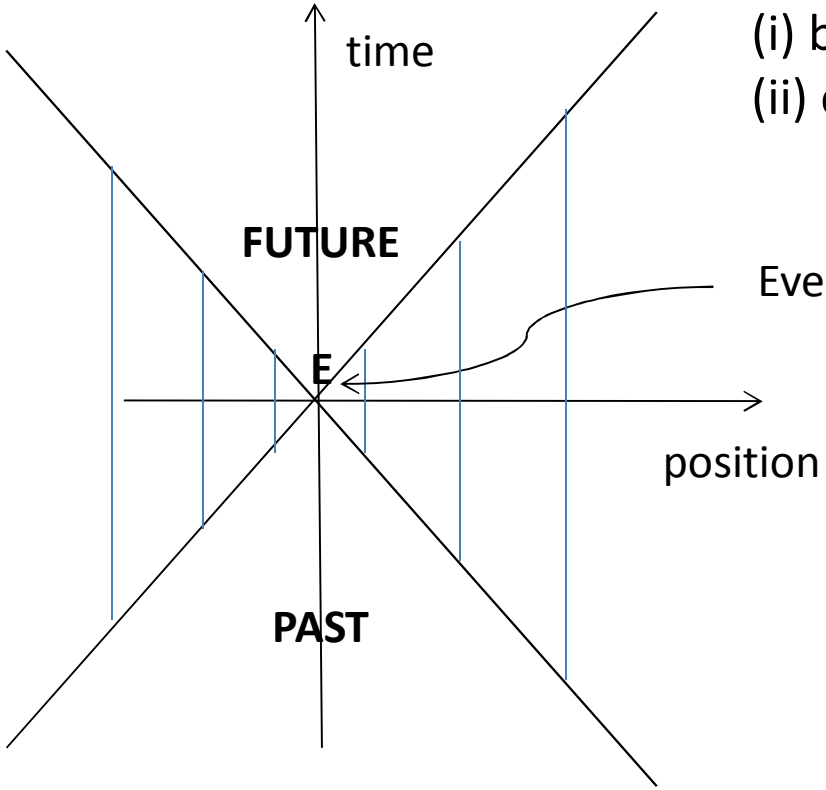
$$\Sigma_B\, q(ab|xy) := q(a|xy) \neq q(a|x)$$

x	a \ y	0	1
0	0	1/2	**2/3**
	1	1/2	**1/3**
1	0	1/2	1/2
	1	1/2	1/2

$$q(a|x0) \neq q(a|x1)$$

Using the box many times Alice can inferr Bob setting y (either 0 or 1) with high probability.

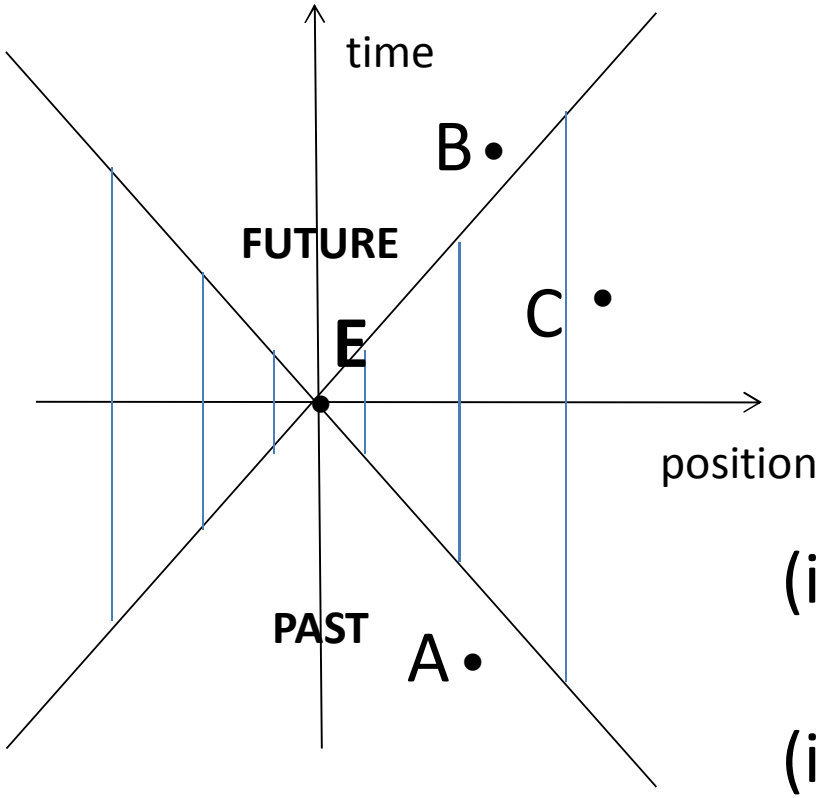
The space-time issue



Event E can:
(i) be casually influenced by its PAST
(ii) casually influence its FUTURE

Event E

The space-time issue



Event E can:
(i) be casually influenced by its PAST
(ii) casually influence its FUTURE

E can

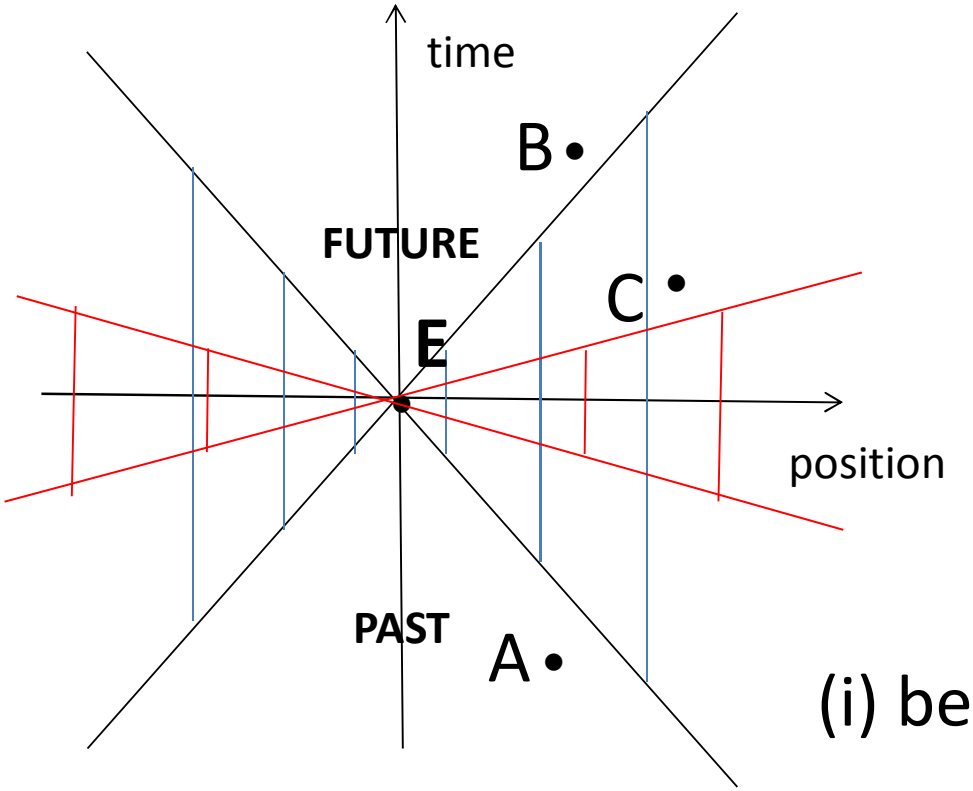
(i) be influenced by A: $E < A$

(ii) influence B: $B < E$

(iii) neither influence
nor be influenced by C: $E \sim C$

What if the speed of light were $v > c_{light}$?

The space-time issue



Event E can:
(i) be casually influenced by its PAST
(ii) casually influence its FUTURE

E can

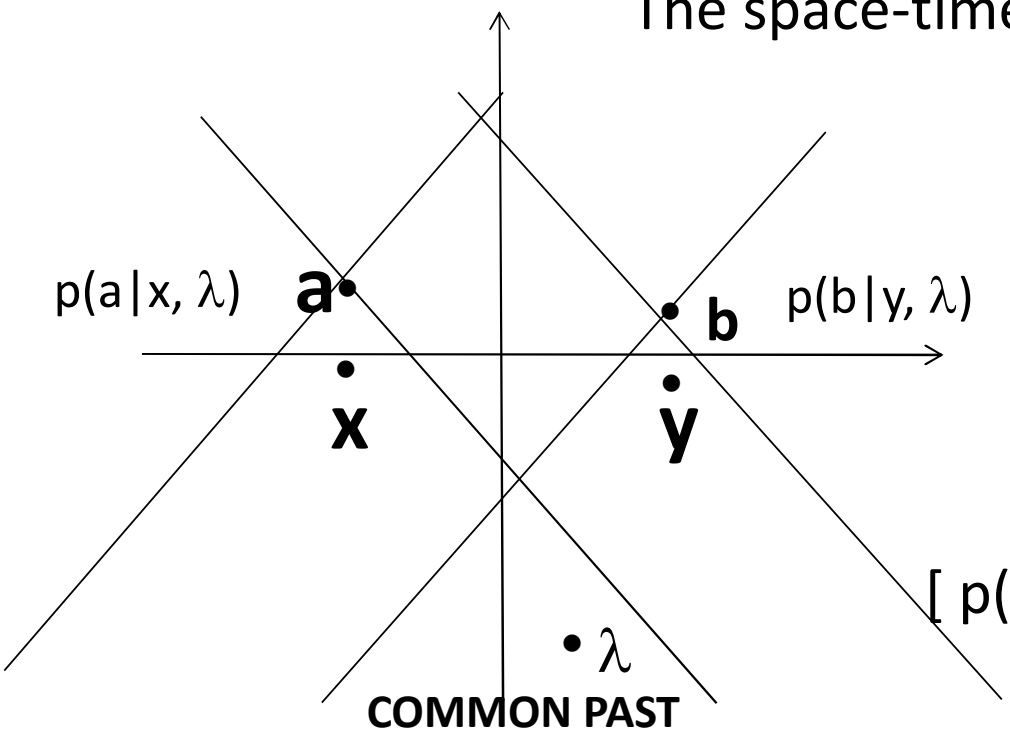
(i) be influenced by A: $E <_v A$

(ii) influence B: $B <_v E$

(iii) influence C: $E <_v C$

$V > C_{light}$

The space-time issue



Generally

$$p(a,b,x,y|\lambda) = p(a,x|\lambda)\, p(b,y|\lambda)$$

Settings x, y before a, b so

$$p(a,b,x,y|\lambda) =$$

$$[\, p(a|x,\lambda)\, \underbrace{p(x|\lambda)}_{p(x)} \,]\, [p(b|y,\lambda)\, \underbrace{p(x|\lambda)}_{p(y)} \,]$$

"Free will" assumption

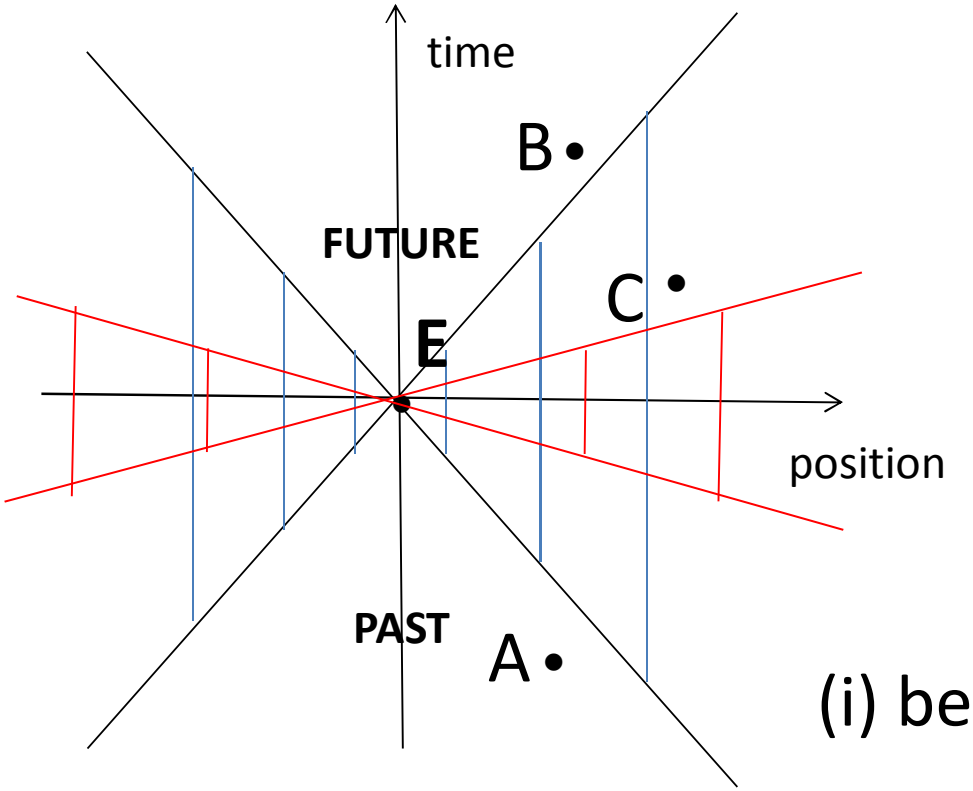
$$p(a,b,x,y|\lambda) = p(a|x,\lambda)\; p(b|y,\lambda)\, p(x)\, p(y)$$ or, after coditioning

$$p(a,b|x,y,\lambda) = p(a,b,x,y|\lambda)/\,[p(x)\, p(y)] = p(a|x,\lambda)\; p(b|y,\lambda)$$

$$p(a,b|x,y) = \Sigma_\lambda\, p(\lambda)\, p(a,b|x,y,\lambda) = \Sigma_\lambda\, p(\lambda)\, p(a|x,\lambda)\; p(b|y,\lambda)$$

(average over λ needed since we do not know its statistics)

The space-time issue



Event E can:
(i) be casually influenced by its PAST
(ii) casually influence its FUTURE

E can

(i) be influenced by A: $E <_v A$

(ii) influence B: $B <_v E$

(iii) influence C: $E <_v C$

$V > C_{light}$

Can quantum statistics be explained locally via some speed $v > c_{light}$?

Cosinder four-party box $p(abcd|xyzw)$

(i) Assume that its BC are locally explained by some superluminal speed $v > c_{light}$ due to $A <_v D <_v B \sim_v C$.

$$p(bc|yz;axdw) = \Sigma_\lambda\, p(\lambda|axdw)\, p(b|y,\lambda)\; p(c|z,\lambda)$$

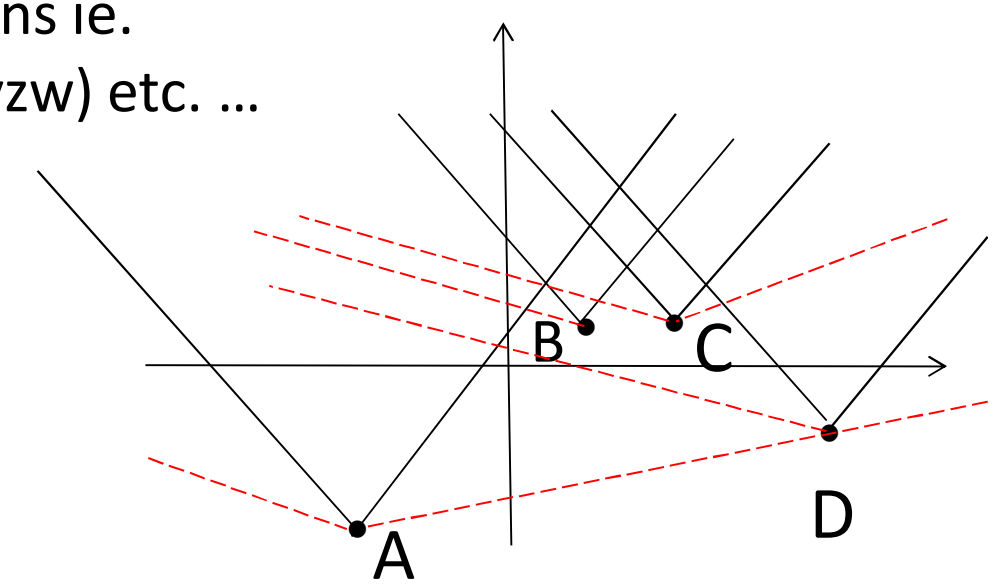
(ii) Assume it satifies NS conditions ie.

$$\Sigma_a\, p(abcd|xyzw)=p(bcd|yzw) \text{ etc. ...}$$

Result. There exists an inequality implied by (i) and (ii) made of correlations ACD, ABD

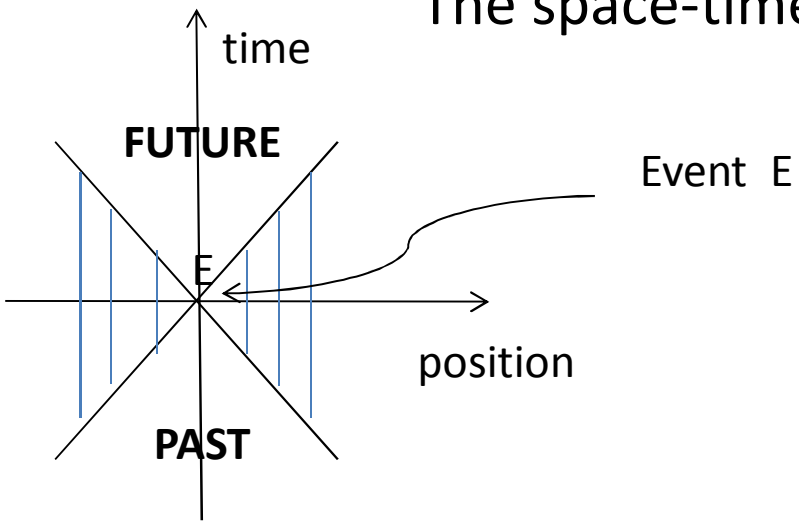
$$S \leq 7$$

however quantum mechanics provides the value $S_Q \approx 7.2$!



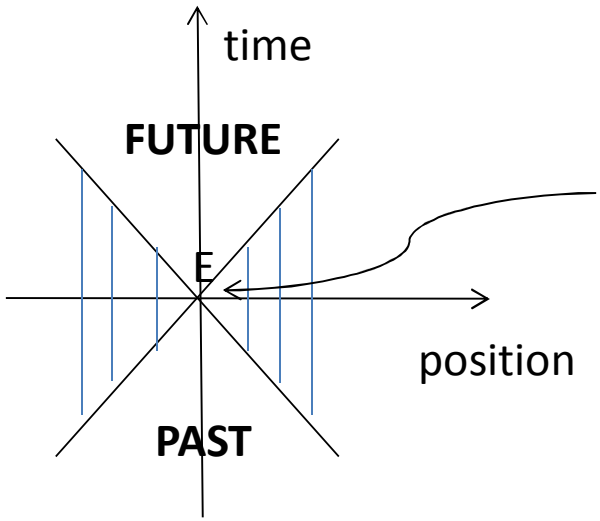
[J. D. Blancal, S. Pironio, A. Acin, Y.-C. Liang, V. Scarani, N. Gisin, Nat. Phys. (2012)]

The space-time issue



Event E

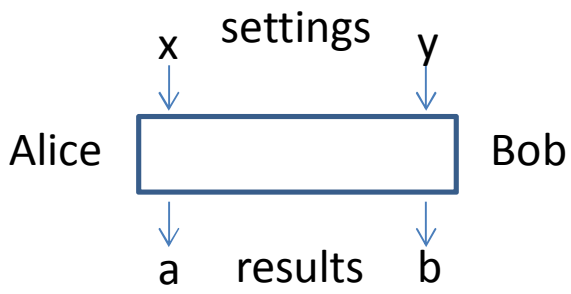
Event E can:
(i) Be influenced by its PAST
(ii) influence its FUTURE



Event E

Theory of no-signaling boxes

[S. Popescu & D. Rohrlich 1994]

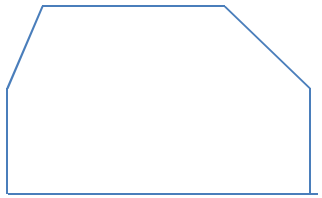


Df. **No-signaling (NS) box:**
family of conditional probability distributions
$\{ p(ab|xy)\}_{ab,xy}$ satisfying no-signaling conditions:

$\Sigma_b p(ab|xy) := p(a|xy) = p(a|x)$ no-signaling from Bob to Alice
(statistics in A does not depend on setting in B)

$\Sigma_a p(ab|xy) := p(b|xy) = p(b|y)$ no-signaling from Alice to Bob
(statistics in B does not depend on setting in A)

Forms the NS polytope – convex set with a facets
and finite number of extremal points.
Central property:
usually not all extremal points deterministic !



Naturally extendable to many parties $\{ p(a_1 \ldots a_n | u_1 \ldots u_n) \}$

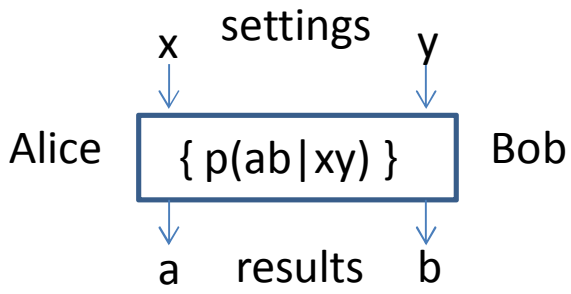
Theory of no-signaling boxes – important subclasses

[S. Popescu & D. Rohlich 1994]

No-signaling (NS) boxes :

$\Sigma_b p(ab|xy) := p(a|xy) = p(a|x)$

$\Sigma_a p(ab|xy) := p(b|xy) = p(b|y)$



Some extremal points deterministic (●) some **nondeterministic** (●) (true origin of randomness).

Quantum (Q) boxes:

$p(ab|xy) = Tr(P_{a,x} \otimes P_{b,y}\, \rho_{AB})$

Local quantum measurements

$\Sigma_a P_{a,x} = I_A, \quad 0 \le P_{a,x} \le I_A$

$\Sigma_b P_{b,x} = I_B, \quad 0 \le P_{b,x} \le I_B$

Usually quantum local observables:

$A_x = \Sigma_a \lambda_{a,x} P_{a,x}$, x – number of the observable $(x=1,\dots,k_A)$

$B_y = \Sigma_a \lambda_{b,y} P_{b,y}$, y – number of the observable $(x=1,\dots,k_B)$

Local hideden variable (LHV) boxes:

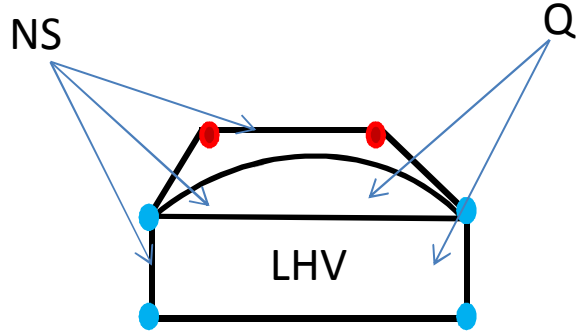
$p(ab|xy) = \Sigma_\omega p(\omega)\, p_\omega(a|x)\, p_\omega(b|y)$,

ω - hidden variable,

$p_\omega(a|x)$, $p_\omega(b|y)$ **can be choosen extremal (deterministic ●)**

eg. for any x, y there are single results $a_{x,\omega}$, $b_{y,\omega}$

s.t. $p_\omega(a_{x,\omega}|x)=1$, $p_\omega(b_{y,\omega}|y)=1$

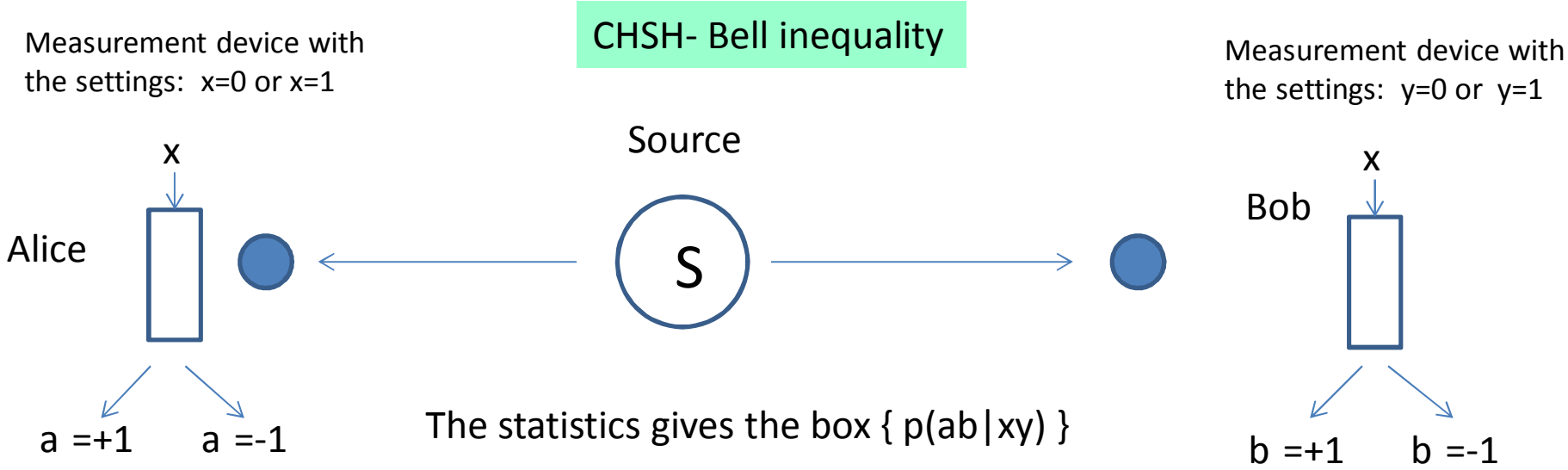


$$\mathbf{LHV \subset Q \subset NS}$$

If the state ρ_{AB} is separable ⇒ Q = LHV.

If the state ρ_{AB} is entangled the sets usually are not equal to each other

CHSH- Bell inequality



Df. Mean value $\langle A_x B_y \rangle = \Sigma_{ab}\, ab\, p(ab|xy)$

Df. Mean value of Bell operator $\langle B \rangle = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle$

Bell inequality: for any LHV boxes one has $\langle B \rangle \leq 2 = C_{LHV}$

Tsirelson bound: for quantum boxes one has $\langle B \rangle \leq 2\sqrt{2} = C_Q$

Algebraic bound:

in general no-signaling theories one has $\langle B \rangle \leq 4 = C_{NS}$

$$C_{LHV} < C_Q < C_{NS}$$

(all the bounds are saturated within the corresponding classes of boxes)

Question.- How the extremal boxes looks like in this CHSH scenario ?

CHSH-Bell inequality (I)

NS = no-signalling polytope

{ p(ab|xy) }– table representations:

x	a \ b \ y	0	1	0	1
0	0	1			1
	1				
1	0	1			1
	1				

Deterministic NS-extremal point.
Generates all NS-extremal points that are LHV.

x	a \ b \ y	0		1	
		0	1	0	1
0	0	1/2		1/2	
	1		1/2		1/2
1	0	1/2			1/2
	1		1/2	1/2	

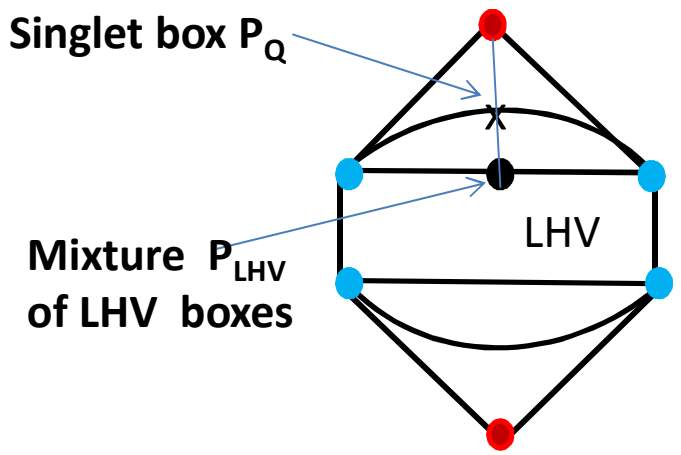
Extremality $\Longrightarrow$ randomness has no correlations with external NS-world (analog of singlet in QM)

Indeterministic NS-extermal points - PR box
Generates all NS-extremal points which are not LHV

x	a \ b	0	1	0	1
0	0	p/2	q/2	p/2	q/2
	1	q/2	p/2	q/2	p/2
1	0	p/2	q/2	q/2	p/2
	1	q/2	p/2	p/2	q/2

$p+q=1$
$p=1/2+\sqrt{2}/4$
$q=1/2-\sqrt{2}/4$

PR-box



Q extremal point – „Singlet box" (generated by the state $|\Psi\rangle=(|0\rangle|0\rangle+|1\rangle|1\rangle)/\sqrt{2}$
(extremal in Q but not in NS !)

CHSH-Bell inequality (II)

x	a \ b	y=0, b=0	y=0, b=1	y=1, b=0	y=1, b=1
0	0	1			1
	1				
1	0	1			1
	1				

$\mathbf{P_{LHV}}$:={ p(a,b|x,y) }

No-signaling LHV-box

x	a \ b	y=0, b=0	y=0, b=1	y=1, b=0	y=1, b=1
0	0		1		1
	1	1		1	
1	0		1	1	
	1	1			1

B:= B(a,b,x,y)

Indicator fuction

x \ y	0	1
0	p_{00}	p_{01}
1	p_{10}	p_{11}

{p(x,y)}

Alice and Bob settings probabilities

x	a \ b	y=0, b=0	y=0, b=1	y=1, b=0	y=1, b=1
0	0		p_{00}		p_{01}
	1	p_{00}		p_{01}	
1	0		p_{10}	p_{11}	
	1	p_{10}			p_{11}

B' := B'(a,b,x,y)

Rescaled indicator fuction

Df. Bell value:

$$\beta=\Sigma_{abxy}\, B(a,b,x,y)\; p(x,y)\; p(a,b|x,y).$$

Alternative formula:

$$\beta=\mathbf{B'.P} = \Sigma_{abxy}\, B'(a,b,x,y)\; p(a,b|x,y)$$

(element-wise multiplication of the tables).

Example. - For the above P_{LHV} the value $\beta = \mathbf{B'.P_{LHV}} = p_{01}$

Thm.- Bell inequality for the settings {p(x,y)}.
Any LHV box must satisfy:

$$\beta \geq \beta_{LHV}=\min_{\{x\,y\}} p(x,y) =\min_{\{x\,y\}} p(x)p(y) \equiv p_{min}$$

Important (!): original CHSH inequality has uniform $\{p(x,y)\}_{xy}$ =)= ½ x ½ =1/4

For application of this mechanism see [A. Grudka et al. arXiv.1303.5591]

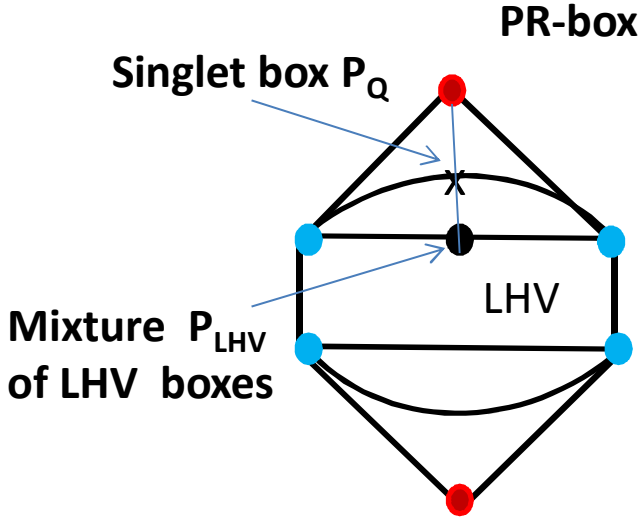
CHSH-Bell inequality (III) – algebraic violation

x	a \ b	y=0, b=0	y=0, b=1	y=1, b=0	y=1, b=1
0	0	1/2		1/2	
	1		1/2		1/2
1	0	1/2			1/2
	1		1/2	1/2	

P_{PR}:={ p(a,b|x,y) }

x	a \ b	y=0, b=0	y=0, b=1	y=1, b=0	y=1, b=1
0	0		p_{00}		p_{01}
	1	p_{00}		p_{01}	
1	0		p_{10}	p_{11}	
	1	p_{10}			p_{11}

B' := B'(a,b,x,y)



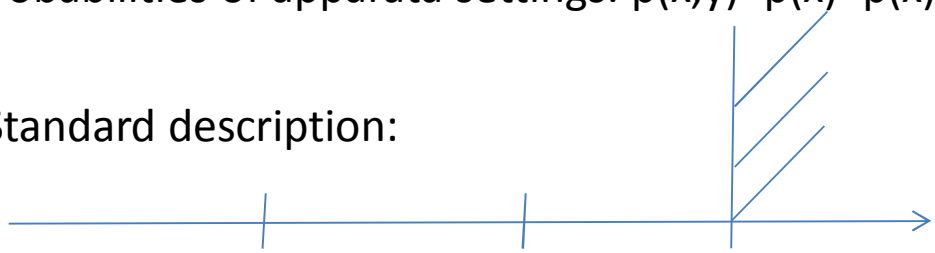
β = **B'.P_{PR} =0 - so called algebraic violation** (since always we must have $\beta \geq 0$)

Theorem.- Only boxes equivalent (up tu permutations) to P_{PR} can violate the above inequality algebraically.

Digression – reverse order of Bell inequality violation

Standard CHSH-Bell inequality
(probabilities of apparata settings: p(x,y)=p(x)=p(x)=1/4 for any x,y)

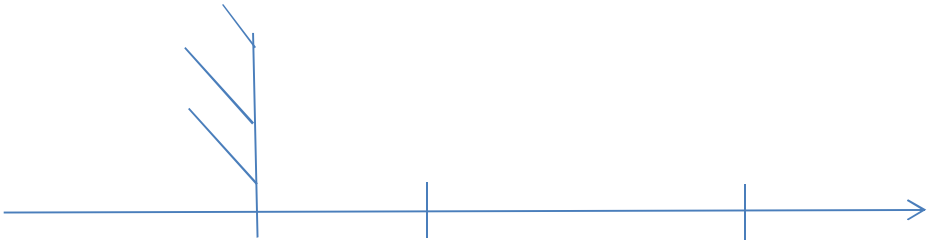
Standard description:



$C_{LHV} = 2$ $C_Q = 2\sqrt{2}$ $C_{NS} = 4$

$\beta = (4-C)/8$

Present description:



$\beta_{NC} = 0$ $\beta_Q = 1/2 - \sqrt{2}/4$ $\beta_{LHV} = 1/4$

$(0 \leq \beta \leq 1)$

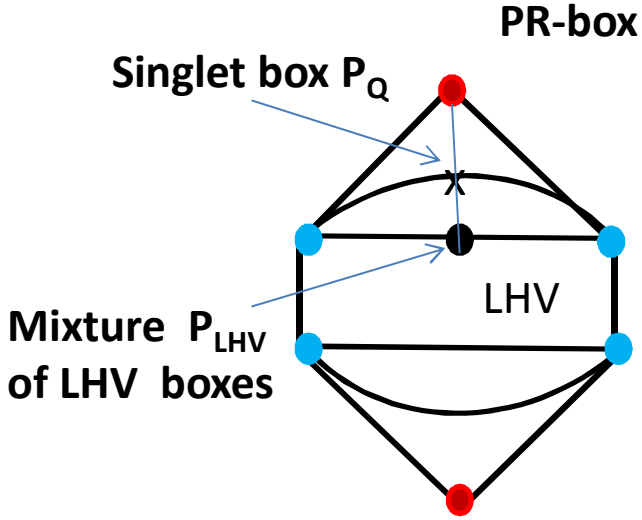
CHSH-Bell inequality (III) – perfect randomness

x \ a \ b \ y	0		1	
	0	1	0	1
0	1/2		1/2	
0		1/2		1/2
1	1/2			1/2
1		1/2	1/2	

P_{PR}:={ p(a,b|x,y) }

x \ a \ b \ y	0		1	
	0	1	0	1
0		p_{00}		p_{01}
0	p_{00}		p_{01}	
1	0	p_{10}	p_{11}	
1	p_{10}			p_{11}

B' := B'(a,b,x,y)



β = **B'.P_{PR} =0 - so called algebraic violation**

Randomness source : Alice and Bob picks up some setting say x=0, y=0 and declare the bit

$$s_r = \begin{cases} 0 & (a,b)=(0,0) \\ 1 & (a,b)\neq(0,0) \end{cases}$$

to be random. Since the box is extremal in NS polytope it is indeed random ie. conditoned upon any external observer guess it satisfies:

$$p(s_r=0|z) = p(s_r=1|z) = ½$$

Question.- How much randomness is in s_r if the box is a mixture of **P_{PR}** and **P_{LHV} ?**

CHSH-Bell inequality (IV) – limits of randomness

Resource: Non-extremal box $P = (1-\gamma)P_{PR} + \gamma\, P_{LHV}$ with known γ

Question: what are the limits of randomness of the bit $s_r = \begin{cases} 0 & (a,b)=(0,0) \\ 1 & (a,b)\neq(0,0) \end{cases}$

Answer: ϵ'-free randomness ie.

$$\tfrac{1}{2} - \epsilon' \leq p(s_r|z) \leq \tfrac{1}{2} + \epsilon'$$

with $\boldsymbol{\epsilon' = \gamma/2}$.

x \ y	a \ b	0	1
0	0	$(1-\gamma)/2 + \gamma\, p(00\|00)$	$\gamma\, p(11\|00)$
	1	$\gamma\, p(11\|00)$	$(1-\gamma)/2 + \gamma\, p(11\|00)$

$$p(s_r=0|z) = (1-\gamma)/2 + \gamma\, p(00|00) \leq$$
$$\leq (1-\gamma)/2 + \gamma \cdot 1 = (1-\gamma)/2$$

(since in LHV one may put $p(00|00)=1$)

Resource: Non-extremal box $P = (1-\gamma)P_{PR} + \gamma\, P_{LHV}$ with unknown γ but known the Bell value $\beta = B' \cdot P$.

Question: the same (limits of randomness of the bit s_r)

Answer.- : ϵ'-free randomness ie.

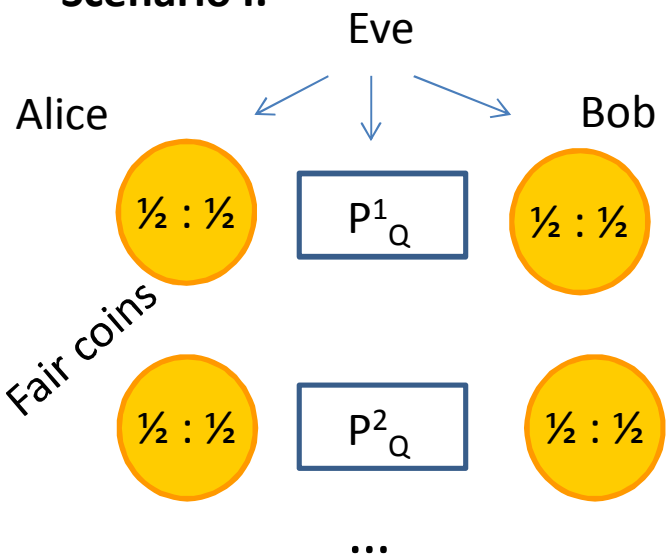
$$\tfrac{1}{2} - \epsilon' \leq p(s_r|z) \leq \tfrac{1}{2} + \epsilon'$$

with $\boldsymbol{\epsilon' = \tfrac{1}{2}\beta/p_{min}}$ where $p_{min} = \min_{\{x\ y\}} p(x,y)$

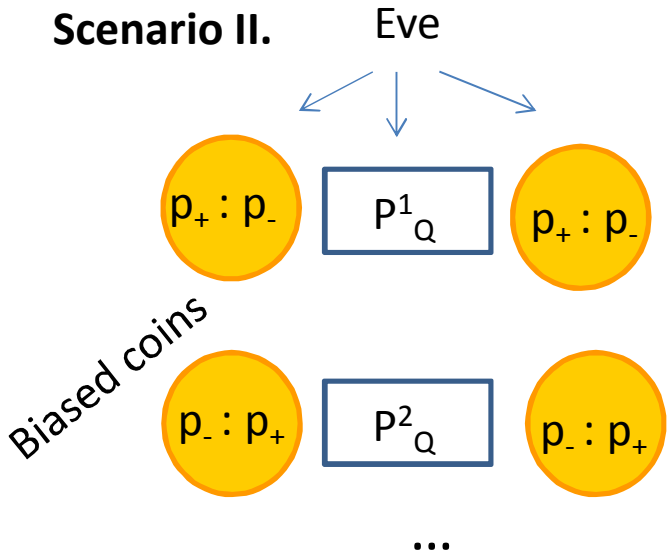
Warning.- It is useless for $\beta \geq p_{min}$ (since always $\epsilon' \leq \tfrac{1}{2}$).
Does it mean that we may loose the randomness of the bit s_r at this point completely ?

CHSH-Bell inequality (IV) – limits of randomness

Scenario I.



Scenario II.



The bias $p_\pm = ½ \pm \epsilon$

ϵ adjusted so that

$\beta_{singlet} = p_{min} := (½ - \epsilon)^2$

Observed Bell value for singlet box:

$\beta_{singlet} = 1/2 - \sqrt{2}/4$

$p_{min} = \min_{\{x\ y\}} p(x,y) = ½ \times ½ = 1/4$

prtially free randomness

$½ - \epsilon' \leq p(s_r|z) \leq ½ + \epsilon'$

with $\epsilon' = ½\,\beta/p_{min} = 1 - 1/\sqrt{2} \approx 0.293$

However it this experiment the value p_{min} can be achieved by deterministic LHV boxes !

„Rectangles'' strategy: always use rectangle representing deterministic LHV model – that overloaps with 1 nonzero element of B' table).

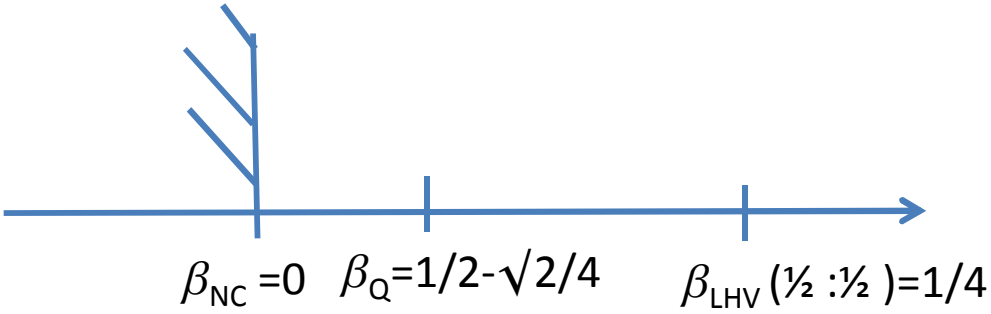
$\beta_{LHV} = \min_{\{x\ y\}} p(x,y) \equiv p_{min} = \beta_{singlet}$

$p(s_r|z) = 0$ or 1 (fully determined by Eve, who correlates boxes with the coins)

Conclusion. – If the settings in Bell experiment are not random enough the deterministic theory may simulate quantum mechanical source !

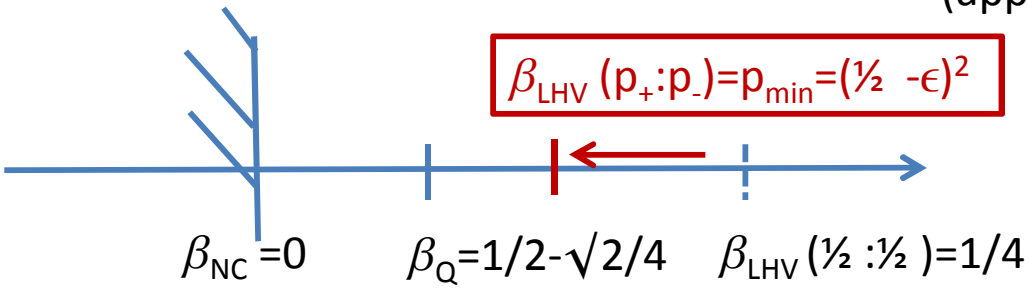
CHSH-Bell inequality (V) – limits of randomness

Scenario I: Standard CHSH-Bell inequality
(probabilities of apparata settings: $p(x,y|\lambda)=p(x|\lambda)=p(x|\lambda)=1/2$ for any x,y)



Scenario II: CHSH-Bell inequality (probabilities of apparata settings **with hidden bias, unknown to Alice and Bob**: $p(x,y|\lambda)=p(x|\lambda)=p(x|\lambda)=p_{\pm}=½\pm\epsilon$ for any x,y)

Remark: $\Sigma\,\lambda\; p(x,y|\lambda)=p(x,y)=1/4$
(apparent full randomness)



At the critical value $\beta_Q=p_{min}=(½-\epsilon)^2$ **there is no randomness (!) in the result since quantum mechaical value is simulated by deterministic LHV theory:** $\beta_Q=p_{min}=\beta_{LHV}$

Amplifying the randomness: the problem.

Natural generalisation of sequence of biased coins
(to include possible memory effects):

$p_+ : p_-$ $\quad p_\pm = ½ \pm \epsilon$

Df. Santha-Vazirani source (called ϵ-SV source).
The source producing an (arbitrary long) string of bits $\{X_1, \ldots, X_n\}$ such that any of its bits conditioned upon its past is ϵ-free:

$$½ - \epsilon \leq p(X_i \mid X_{i-1}, \ldots, X_1) \leq ½ + \epsilon$$

Theorem.- [M. Santa, U. Vazirani, (1984)] There is no classical deterministic function that would produce from ϵ-SV source the bit that is ϵ'-free with $\epsilon' < \epsilon$.

For characterisation of extremal poits of ϵ-SV see [A. Grudka et al. arXiv.1303.5591]

Questions.- (see [D. Collbeck, R. Renner Nature Physics (2012)])
(A) Is it possible to beat the above no-go result with help of quantum mechanics ?
(A') More precisely: starting form given ϵ-SV ($0 < \epsilon < 1/2$) and some quantum states can one produce bit that is ϵ'-free for arbitrary small ϵ' ?
(B) What is the range of the values of the initial ϵ that allow for the latter ?
Is it possible for arbitrary weak initial randomness (ϵ arbitrary close to ½) ?

Observation .- (limitation to (B))
Consider the inequality that is algebraically violated in theory of NS boxes ie. $\beta_{NS} = 0$.
Then it is impossible to success for arbitrary weak initial ϵ unless one has $\beta_{QM} = 0$ as well.

Free randomness problem – the intution

Imagine absent minded scientist who every day goes to a restaurant with the description of ,,Recomendation of the day'' visible in front of it. Suppose that the scientics every day see the description but does not notice. Simply his consciousness doe not register it. But suppose that the subconsciousness does. As a result every day he pick up the dish with the conditional probability

$$\Pr(\text{ choice } | \text{ recommendation of the day }) = 1/2 + \epsilon \approx 1 \quad (*)$$

(say ϵ=0.99 x ½) . Since the restaurant picks the recommendation of the day randomly (and all its offers taste very well) on average the scientist may belive that he uses his free will in choosing his lunch. But obvoiusly he is not.

Suppose that he had been given the source of ,,free randomness'' ie. the one producing certified string of bits that are **,,freely random'' ie. 50:50 random and completely uncorrelated with the rest of the world.** Then he may take a choice that is completely independent on the restaurant's recommendation. However no such source is proven to exists on the market (problem of superdeterminism).

Question: given a little source of its own every day ϵ-free randomness (*) and laws of quantum mechanics is there a chance that some day he will pick his lunch (almost) completely independently on the recommendation ?

Amplifying randomness – general scenario

Eve

Alice $\{ p(\mathbf{ab}e|\mathbf{xy}w) \}$ Bob $\nu^{\epsilon}_{w,e}(\mathbf{r})$ E - single bit (Eve's guess)

Single NS box (many uses forward signaling) **ϵ-SV source: input ϵ-free-randomness**

Pr ≈ 1

$$\tfrac{1}{2} - \epsilon' \leq p(s|e,w) \leq \tfrac{1}{2} + \epsilon'$$

output ϵ'-free random bit

Goal: Given ϵ produce **arbitrary small ϵ' (equiv. – reproduce all ϵ'-s $0 < \epsilon' < \epsilon$).**
Possible modification: many devices NS w. r. to each other
Tool: monogamy/extremality of ,,nonlocal ''(not-LHV) correlations revealed by Bell inequality violation

Fundamental assumption: The Alice and Bob box $\{ p(\mathbf{ab}|\mathbf{xy}) \}$ (traced out over Eve degrees) MUST be produced by Quantum Theory:

$p(ab|xy) = \mathrm{Tr}(P_{a,x} \otimes P_{b,y}\, \rho_{AB})$ for some state ρ_{AB} and local measurements $\{P_{a,x}\}$, $\{P_{b,y}\}$.

Interpretation: Only laws of Quantum Theory are seen in Alice and Bob labs.

Amplifying randomness against no-signalling adversary – summary

(I) [Renner, Collbeck, N. Phys. 2012] (pioneering):

- single device,
- treshold $\epsilon < \epsilon_0$ for initial ϵ
- 2-qubit chain Bell inequality (algebraic violation $\Rightarrow$ full randomness)

Comment: originally working for $\epsilon < 0.081$, proven not to work for $\epsilon > 0.14$.
Exact (,,if and only if'') treshold found to be $\epsilon_0 = 0.091$ (see [A. Grudka et al. arXiv.1303.5591])

(II) [R. Gallego *et al.* arXiv.1210.6514]:

- unbounded number of devices ($n(\epsilon, \epsilon') \longrightarrow \infty$ with $\epsilon' \longrightarrow 0$) ,
- works for all initial $0 < \epsilon < ½$ (arbitarly small initial randomness)
- 5 qubit Mermin inequality (algebraic violation gives partial randomness)
- hash function applied which is only existentially known (not explicit)
- no explicit noise tollerance.

(III) This work [R. Ramanathan *et al.* arXiv.1308.4635]:

- unbounded number of devices as above,
- works for all initial $0 < \epsilon < ½$ (arbitarly small initial randomness).
- 4 qubit Mermin inequality (algebraic violation gives partial randomness),
- explicit hash function (XOR),
- noise tolerance,
- extra tool: de Finetti theorem for SV source and memory.

Remark .- Amplification of randomness against quantum adversary:
single device, no treshold, three qubits [M. Pawłowski, P. Mironowicz, arXiv-1301.7722]

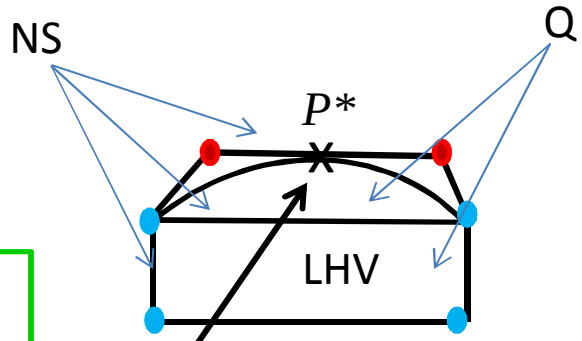
Prelude (I): 4-qubit Bell inequality – the structure

$P(\mathbf{x}|\mathbf{u}) := P(x_1,x_2,x_3,x_4|u_1,u_2,u_3,u_4)$, $x_i,u_i \in \{0,1\}$ (binary settings, binary outcomes)

$$B(\mathbf{x},\mathbf{u}) = \mathrm{I}_{\oplus_{i=1}^4 x^i=0}\ \mathrm{I}_{\mathbf{u}\in\mathbf{U}_0} + \mathrm{I}_{\oplus_{i=1}^4 x^i=1}\ \mathrm{I}_{\mathbf{u}\in\mathbf{U}_1}$$

$$\mathbf{U}_0 = \{\{0001\},\{0010\},\{0100\},\{1000\}\}$$

$$\mathbf{U}_1 = \{\{0111\},\{1011\},\{1101\},\{1110\}\}$$



Bell inequality: for any LHV box $P(\mathbf{x}|\mathbf{u})$ one has:

$$\mathbf{B}.\{P(\mathbf{x}|\mathbf{u})\} = \sum_{\mathbf{x},\mathbf{u}} B(\mathbf{x},\mathbf{u})P(\mathbf{x}|\mathbf{u}) \geq 2 \ (=\beta_{\mathrm{LHV}})$$

(Rather rare phenomenon, see however R. Gallego et al. arXiv:1210.6514] for 5-qubit case)

Quantum violation: there is a 4-qubit quantum state $|\Psi\rangle$ and binary measurements ,,producing'' the **quantum (Q) box** $P^*(\mathbf{x}|\mathbf{u})$ which **violates the inequality algebraically**

$$\mathbf{B}.\{P^*(\mathbf{x}|\mathbf{u})\}=0 \ (=\beta_{\mathrm{Q}}=\beta_{\mathrm{NS}})$$

4-qubit state:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\phi_-\rangle|\tilde{\phi}_+\rangle + |\psi_+\rangle|\tilde{\psi}_-\rangle)$$

$$|\phi_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle)$$

$$|\psi_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle)$$

Measurements for each (i-th) qubit:

$u_i=0$ - measure σ_z

$u_i=1$ - measure σ_x

$$\left.\begin{array}{l}|\tilde{\phi}_+\rangle \\ |\tilde{\psi}_-\rangle\end{array}\right\}$$

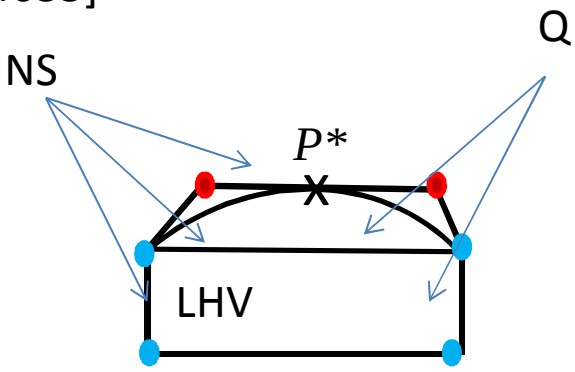
2-nd qubit

$|\pm\rangle=(|0\rangle\pm|1\rangle)/\sqrt{2}$

Prelude (II) : Bell inequality – guarantee of randomness (not automatic)

[R. Ramanathan *et al.* arXiv.1308.4635]

Potential problem: quantum box $P^*(\mathbf{x}|\mathbf{u})\}$ is the mixture of extremal NS boxes P^1_{NS}, é P^r_{NS} violating the inequality maximally.
There may be no setting **u*** with the outcome binary fuction $s_{\mathbf{u}^*}(\mathbf{x})$ **that produces the random bit for all** P^1_{NS}, é P^r_{NS} . For any particular preegreed setting **u*** Eve might sent just the particular box P^1_{NS} that does not have randomness in that setting.



(Rather rare phenomenon, see however R. Gallego et al. arXiv:1210.6514] for 5-qubit case and M. Pawłowski,P. Mironowicz arXiv-1301.7722)

Lemma.- Suppose $\mathbf{B}.\{P(\mathbf{x}|\mathbf{u})\} = \delta \leq 5/7 < 2 = \beta_{\mathrm{LHV}}$ then **for any** measurement setting **u** the function $s_{\mathbf{u}}(\mathbf{x}) := s_{\mathbf{u}}(x_1,x_2,x_3,x_4) = \mathrm{maj}(x_1,x_2,x_3)$ produces the random bit with the bias

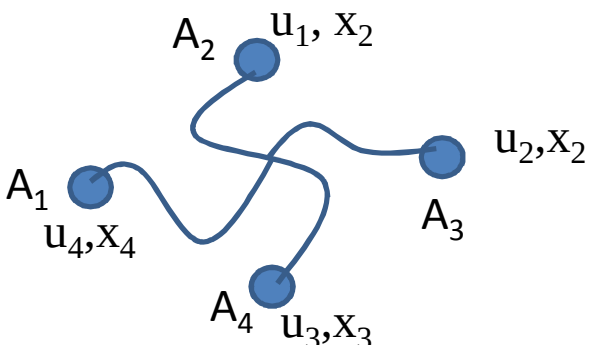
$$\epsilon \leq [11 + 7\,\delta]/32.$$

The 4-qubit protocol – iid. amplification of nonideal randomness

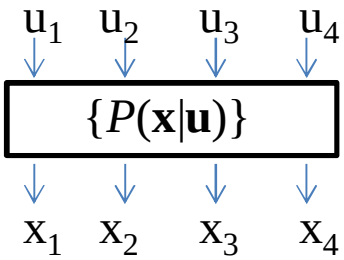
[R. Ramanathan *et al.* arXiv.1308.4635]

Assumption: Bell value known a priori

Entangled 4-qubit in state $|\Psi\rangle$,
u=0 - measure σ_z , u=1 - measure σ_x



$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\phi_-\rangle|\tilde{\phi}_+\rangle + |\psi_+\rangle|\tilde{\psi}_-\rangle)$$

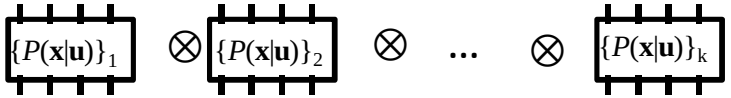


Algebraic violation $\boldsymbol{B}.P=0$

$s_u(\mathbf{x})$:= maj(x_1,x_2,x_3) is an ϵ-bit with ϵ = 11/32
(not perferct ϵ=0 !)

Lemma.- If the state/box noisy, has say
$$\boldsymbol{B}.P < \delta < 5/6$$
then the bit $s_u(\mathbf{x})$:= maj(x_1,x_2,x_3) is ϵ-random with some ϵ = [11/16 + 7 δ/16]/2 < ½

Assumption: an ,,iid'' source (equvalent to the measurements on $|\Psi\rangle^{\otimes k}$):



$(s_1, s_2, \ldots, s_k)$ - k bits, product, at least ϵ-random ie.

$(p_1,1-p_1) \otimes (p_2,1-p_2) \otimes \ldots \otimes (p_k,1-p_k)$ with

$½ - \epsilon_i \leq p_i \leq ½ + \epsilon_i$, i=1,…,k, $\epsilon_i \leq \epsilon < ½$

Lemma.- XOR function $s_r = \oplus_i s_i$ of ϵ_i – random bits s_i is ϵ'-random with $\epsilon' \leq ½ \prod_{i=1}^{k} (2\,\epsilon_i)$. $\xrightarrow[k\to\infty]{} 0$

The XOR bit s_r is ϵ'-random with arbitrary small ϵ'

The 4-qubit protocol – full description (I)

[R. Ramanathan *et al.* arXiv.1308.4635]

Problems with the previous protocol

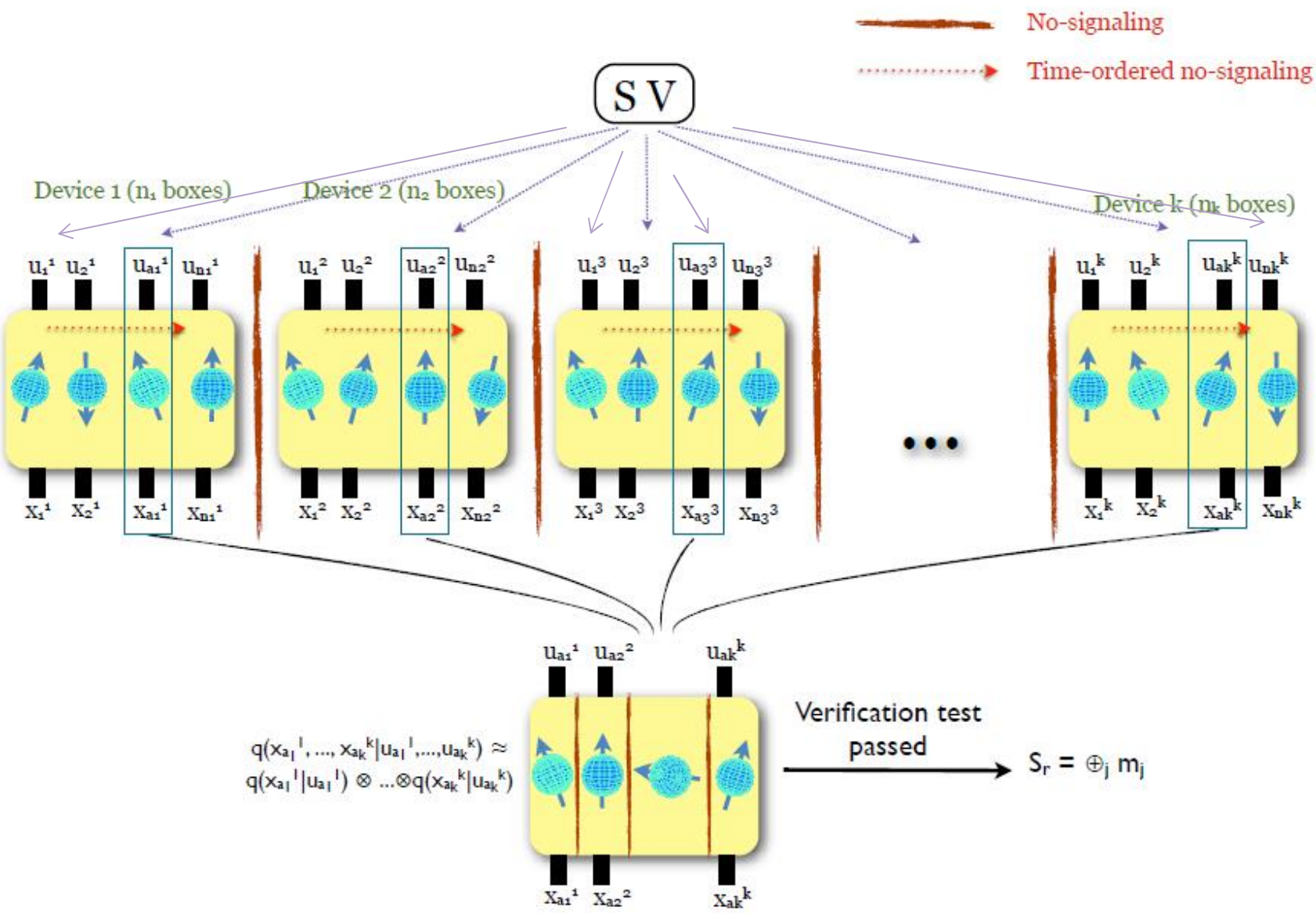
1) Assumption that **Bell value is a priori known - not justified**
2) **iid. (product, indentical)** assumption **may not be true**
3) **estimation of Bell value may suffer form**
   (i) **non iid. character**
   (ii) **weak free randomness (only ϵ -SV source)**

Given 4M devices (quantumly: M 4-qubit systems) expected to violate approximately the Bell inequality the protocol below is applied.

Protocol

1. The ε-SV source generates $4M$ bits which are used by the parties to choose the measurement settings $\mathbf{u}^1_{\leq m_1}, \ldots, \mathbf{u}^k_{\leq m_k}$ for the $4k$ devices, where $M = \sum_{j=1}^k m_j$. The measurements are performed sequentially on each device. The devices produce the output bits $\mathbf{x}^1_{\leq m_1}, \ldots, \mathbf{x}^k_{\leq m_k}$. After the measurements, the parties discard the settings that do not appear in the Bell inequality in Eq. (5) and a number n_j of runs remain in the j-th device for $1 \leq j \leq k$.
2. The parties choose one box a_j from each device using $\log n_j$ bits from the ε-SV source, for $1 \leq j \leq k$.
3. The parties perform an estimation of the violation of the Bell inequality in the chosen boxes by computing the empirical average $Z_k := \frac{1}{k}\sum_{i=1}^k B(\mathbf{x}_{a_i}, \mathbf{u}_{a_i})$. The protocol is aborted unless $Z_k \leq \left(\frac{1}{2} - \varepsilon\right)^4 \frac{\delta}{2}(1-\mu)$ (with fixed constants δ, μ).
4. Conditioned on not aborting in the previous step, the parties compute $m_j := \mathrm{maj}(x_j^1, x_j^2, x_j^3)$ for all $1 \leq j \leq k$, and output the bit $S_r = \oplus_{j=1}^k m_j$.

The 4-qubit protocol – full description (II)



De Finetti –type theorem

Lemma 6. *Let $P(x^1_{\leq n_1}, \ldots, x^k_{\leq n_k} | u^1_{\leq n_1}, \ldots, u^k_{\leq n_k})$ be a time-ordered non-signaling distribution, with output and input alphabets Σ and Λ, respectively (i.e. $P : \Sigma^{\times n} \times \Lambda^{\times n} \to \mathbb{R}^+$). The distribution P represents k devices each with n_j boxes. Let $(a_1, \ldots, a_k) \in [n_1] \times \ldots \times [n_k]$ and $(u^1_{\leq n_1}, \ldots, u^k_{\leq n_k})$ be chosen from an ε-SV source $\nu(a_1, \ldots, a_k, u^1_{\leq n_1}, \ldots, u^k_{\leq n_k})$.*

Then for every set of positive reals $\{t_2, \ldots, t_k\}$,

$$\Pr_{(a_1,\ldots,a_k)\sim\nu} \left(T \geq \sum_{i=2}^{k} \sqrt{\frac{8 \ln(2) t_i^2 \sum_{j=1}^{i-1} n_j}{n_i^{1-\log(1+2\varepsilon)}}} \right) \leq \sum_{i=2}^{k} \frac{1}{t_i}, \tag{33}$$

with

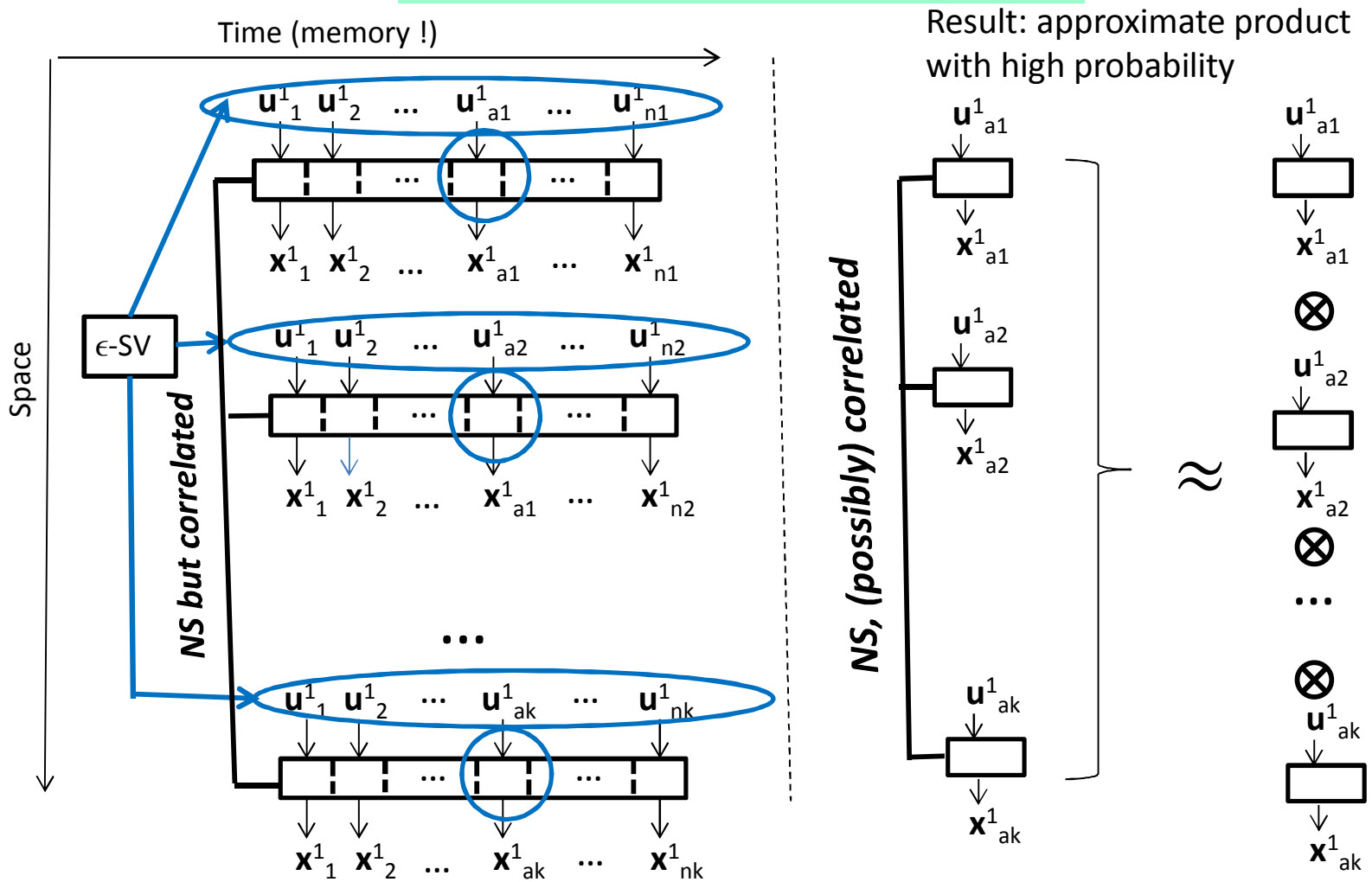
$$T := \mathbb{E}_{u^1_{\leq n_1}, \ldots, u^k_{\leq n_k} \sim \nu_{a_1,\ldots,a_k}} \quad \mathbb{E}_{x^1_{<a_1}, \ldots x^k_{<a_k} \sim P} \left\| q(x^1_{a_1}, \ldots, x^k_{a_k} | u^1_{a_1}, \ldots, u^k_{a_k}) - q(x^1_{a_1} | u^1_{a_1}) \otimes \ldots \otimes q(x^k_{a_k} | u^k_{a_k}) \right\|_1 \tag{34}$$

where q is the conditional box given the inputs $u^j_{<a_j}$ and outputs $x^j_{<a_j}$ for all $1 \leq j \leq k$

$$q(x^1_{a_1}, \ldots, x^k_{a_k} | u^1_{a_1}, \ldots, u^k_{a_k}) := P_{\substack{x^1_{<a_1}, \ldots, x^k_{<a_k} \\ u^1_{<a_1}, \ldots, u^k_{<a_k}}} (x^1_{a_1}, \ldots, x^k_{a_k} | u^1_{a_1}, \ldots, u^k_{a_k}), \tag{35}$$

and $\nu_{a_1,\ldots,a_k}$ is the probability ν conditioned on measuring $(a_1, \ldots, a_k)$.

De Finetti – type theorem - conclusion



Conclusion.- If $n_1 = 1, \quad n_i^{1-\log(1+2\varepsilon)} = 8\ln(2)k^2t^3 n_{i-1}$ then

$$\Pr\left\{ \left\| q(\mathbf{x}^1_{a_1},\ldots,\mathbf{x}^k_{a_k}|\mathbf{u}^1_{a_1},\ldots,\mathbf{u}^k_{a_k}) - q(\mathbf{x}^1_{a_1}|\mathbf{u}^1_{a_1}) \otimes \ldots \otimes q(\mathbf{x}^k_{a_k}|\mathbf{u}^k_{a_k}) \right\|_1 \leq O(1/\sqrt{t}) \right\} \geq 1 - O(1/\sqrt{t})$$

where $q(x^1_{a_1},\ldots,x^k_{a_k}|u^1_{a_1},\ldots,u^k_{a_k}) := P_{\substack{x^1_{<a_1},\ldots,x^k_{<a_k} \\ u^1_{<a_1},\ldots,u^k_{<a_k}}}(x^1_{a_1},\ldots,x^k_{a_k}|u^1_{a_1},\ldots,u^k_{a_k})$.

Estimation of Bell inequality

$$q(\mathbf{x}^1_{a_1},\ldots,\mathbf{x}^k_{a_k}|\mathbf{u}^1_{a_1},\ldots,\mathbf{u}^k_{a_k}) \longrightarrow P(\mathbf{x}_1,\ldots,\mathbf{x}_k|\mathbf{u}_1,\ldots,\mathbf{u}_k)$$

Df. The NS-box $P(\mathbf{x}_1,\ldots,\mathbf{x}_k|\mathbf{u}_1,\ldots,\mathbf{u}_k)$ is **(μ,δ)-good** iff there exists subset A $\subset$ {1,…,k}, |A| > μk such that $\mathbf{B}.\{P_{\substack{\mathbf{x}_1,\ldots,\mathbf{x}_{l-1}\\ \mathbf{u}_1,\ldots,\mathbf{u}_{l-1}}}(\mathbf{x}_l|\mathbf{u}_l)\} < \delta$ where $P_{\substack{\mathbf{x}_1,\ldots,\mathbf{x}_{l-1}\\ \mathbf{u}_1,\ldots,\mathbf{u}_{l-1}}}(\mathbf{x}_l|\mathbf{u}_l)$ is P conditioned upon the ,,l-1 history''.

Interpretation: more than μk (coditioned) boxes have Bell value $\mathbf{B}.P$ smaller than $\boldsymbol{\delta}$.
(Remember: the smaller Bell value the better since $\mathbf{B}.P$=0 gives algebraic violation and the best randomness possible in this scheme).

Df. The protocol **accepts iff** the empirical value $Z_k := \frac{1}{k}\sum_{l=1}^{k} B(\mathbf{x}_l,\mathbf{u}_l)$ (with the settings $\mathbf{u_1,\ldots,u_k}$ choosen according to the ϵ-SV-source) satisfies $Z_k \leq \left(\frac{1}{2}-\varepsilon\right)^4 (1-\mu)\frac{\delta}{2}$.

Lemma. The conditional probability of acceptance Pr(reject|not (μ,δ)-good) satisfies Pr(reject | not (μ,δ)-good) $\geq$ 1- c^{-1} exp[-k(½- ϵ)^8 (1-μ)$^2\delta^2$]

Conclusion.- If Pr(accept) > c (ie. it is finite) then

Pr((μ,δ)-good|accept) $\geq$ 1- c^{-1} exp[-k(½- ϵ)^8 (1-μ)$^2\delta^2$]

(intepretation: the accepted boxes are with high probability (μ,δ)-good) .

Puting the things together (I)

Combining the conditional acceptance probability , probability of the succes in de Finetti (productness) , the XOR property and the linear programing bound gives eventually:

Proposition.- If Pr(*accept*) > c (finite) the 4-qubit protocol provides with the probability $\Pr \geq 1 - O(1/\sqrt{t}) - c^{-1} \exp[-k(\tfrac{1}{2} - \epsilon)^8 (1-\mu)^2 \delta^2] \xrightarrow[t \to \infty]{k \to \infty} 1$ the ϵ'-random box satisfying:

$$0 \leq \epsilon' \leq f(\epsilon, \delta, \mu, k, t) \xrightarrow[t \to \infty]{k \to \infty} 0 \text{ for any } 0<\mu<1,\ 0 \leq \delta < 5/7 \text{ and } \mathbf{0 \leq \epsilon < 1/2}$$

Here $f(\epsilon, \delta, \mu\ k, t) := ([11 + 7\,\delta]/16)^{\mu k} + c^{-1} \exp[-k(\tfrac{1}{2} - \epsilon)^8 (1-\mu)^2 \delta^2] + O(1/\sqrt{t})$.

Question .- *Is it possible that quantum mechanics guarantees the finite Pr(accept) ?*

(You might have it only by some unlikely long range fluctuations, while here we want the probability to be independent on k in the limit).

Puting the things together (II)
Application of Quantum Mechanics

Question.- *Is it possible that quantum mechanics guarantees the finite Pr(accept) ?*

Answer: YES

Proposition.-

Suppose that we apply the above protocol to the box $P(\mathbf{x}_1, \ldots, \mathbf{x}_k | \mathbf{u}_1, \ldots, \mathbf{u}_k)$ that is (1, δ')-good. Then one has Pr(accept) $\geq 1 - \exp\left(-\frac{k(1/2-\varepsilon)^8(1-\mu)^2\delta^2}{2048}\right)$

as long as $\delta' \leq \frac{(1-\mu)\delta(\frac{1}{2}-\varepsilon)^4 f(\varepsilon)}{4(\frac{1}{2}+\varepsilon)^4}$ $\approx$ $O(\delta(1-\mu)(1-2\varepsilon)^4)$.

Here $f(\varepsilon) := \left(\frac{1}{2}+\varepsilon\right)^4 + \left(\frac{1}{2}-\varepsilon\right)^4 + 4\left(\frac{1}{2}-\varepsilon\right)^3\left(\frac{1}{2}+\varepsilon\right) + 2\left(\frac{1}{2}-\varepsilon\right)^2\left(\frac{1}{2}+\varepsilon\right)^2$

Quantum realisation:

(approximate) quantum iid. source with k mixed 4-qubit states of the form $(1- 16\delta')|\Psi\rangle\langle\Psi| + \delta' I^{\otimes 4}/16$.

Open problems

1) Improve scaling.

2) Finite number of devices that would work for arbitrary weak
(but not completely deteministic) ϵ-SV source ?
(i) Weak version: $n(\epsilon, \epsilon')= n(\epsilon)$ (increases only with the input - ϵ going down,
but for fixed input- ϵ it is just some finite number of devices)
(ii) Strong version: $n(\epsilon, \epsilon')\leq n_0$ (far conceptual extension along lines of [R. Colbeck & R. Renner 2012])

3) Any arbitrary weak (but not completely deteministic) ϵ-SV
source randomness amplification based on bipartite quantum state ?

4) Is there any chance to improve de Finetti-type theorem. What are
its limits in the case of ϵ-SV application ?

5) Are there finite rates possible (in terms of number of the devices or uses (?))
for arbitary small randomness ?

6) Amplification form other sources like a min entropy one ?

Remark.- *Some progress in context of the above questions will be provided soon ([F. G. S. L. Brandao, R.Ramanathan, A. Grudka, K. Horodecki, M. Horodecki, P. H., coming soon …]).*
In particular : finite number of devices (three) is enough (!).

Summary

- First fully constructive proof that quantum mechanics allows for device independent (ie. against general no-signalling adversaries) amplification of arbitrary weak randomness (ϵ-SV source)

- Simple explicit hashing function (XOR)

- Finite noise – tollerance

- Estimation of Bell inequality with memory (,,1-way signaling'')

- de Finetti-type theorem with ϵ-SV source (of independent interest)

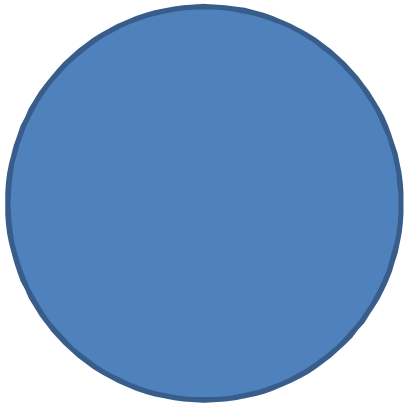
Krajowe Centrum Informatyki Kwantowej

National Quantum Information Centre of Gdańsk (NQuantIC)

ul. Wł. Andersa 27
81-824 Sopot

http://www.kcik.univ.gda.pl/

Single (physical) source of 4-qubit entanglement:
Bell inequality violation leading to linear min-entropy (statistical) source



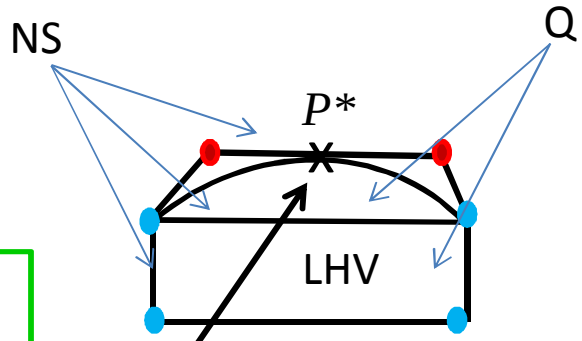
Prelude (I): 4-qubit Bell inequality – the structure

$P(\mathbf{x}|\mathbf{u}) := P(x_1,x_2,x_3,x_4|u_1,u_2,u_3,u_4)$, $x_i,u_i \in \{0,1\}$ (binary settings, binary outcomes)

$$B(\mathbf{x},\mathbf{u}) = \mathrm{I}_{\oplus_{i=1}^4 x^i=0}\ \mathrm{I}_{\mathbf{u}\in\mathbf{U}_0} + \mathrm{I}_{\oplus_{i=1}^4 x^i=1}\ \mathrm{I}_{\mathbf{u}\in\mathbf{U}_1}$$

$$\mathbf{U}_0 = \{\{0001\},\{0010\},\{0100\},\{1000\}\}$$

$$\mathbf{U}_1 = \{\{0111\},\{1011\},\{1101\},\{1110\}\}$$



Bell inequality: for any LHV box $P(\mathbf{x}|\mathbf{u})$ one has:

$$\mathbf{B}.\{P(\mathbf{x}|\mathbf{u})\} = \sum_{\mathbf{x},\mathbf{u}} B(\mathbf{x},\mathbf{u})P(\mathbf{x}|\mathbf{u}) \geq 2 \ (=\beta_{\mathrm{LHV}})$$

(Rather rare phenomenon, see however R. Gallego et al. arXiv:1210.6514] for 5-qubit case)

Quantum violation: there is a 4-qubit quantum state $|\Psi\rangle$ and binary measurements ,,producing'' the **quantum (Q) box** $P^*(\mathbf{x}|\mathbf{u})$ which **violates the inequality algebraically**

$$\mathbf{B}.\{P^*(\mathbf{x}|\mathbf{u})\}=0 \ (=\beta_{\mathrm{Q}}=\beta_{\mathrm{NS}})$$

4-qubit state:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\phi_-\rangle|\tilde{\phi}_+\rangle + |\psi_+\rangle|\tilde{\psi}_-\rangle)$$

$$|\phi_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle)$$

$$|\psi_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle)$$

Measurements for each (i-th) qubit:

$u_i=0$ - measure σ_z

$u_i=1$ - measure σ_x

$$\left.\begin{array}{l}|\tilde{\phi}_+\rangle \\ |\tilde{\psi}_-\rangle\end{array}\right\}$$

2-nd qubit

$|\pm\rangle=(|0\rangle\pm|1\rangle)/\sqrt{2}$

Facts on single copy boxes

Lemma 1. (comparing averages)

$$\left.\begin{aligned} \overline{B}^U &= \frac{1}{|U|}\mathbf{B}.\{P(\mathbf{x}|\mathbf{u})\} = \frac{1}{|U|}\sum_{\mathbf{u},\mathbf{x}} B(\mathbf{x},\mathbf{u})P(\mathbf{x}|\mathbf{u}) \quad \text{(fair conis)} \\ \overline{B}^{SV} &= \sum_{\mathbf{u},\mathbf{x}} \nu_{SV}(\mathbf{u})B(\mathbf{x},\mathbf{u})P(\mathbf{x}|\mathbf{u}) \quad \text{(biased conis)} \end{aligned}\right\} \Longrightarrow \frac{1}{(\frac{1}{2}+\varepsilon)^4|U|}\overline{B}^{SV} \leq \overline{B}^U \leq \frac{1}{(\frac{1}{2}-\varepsilon)^4|U|}\overline{B}^{SV}$$

Proof. – Obvious.

Lemma 2. (randomness with fair coins quaranteed for any setting and outcomes)

$$\overline{B}^U := \frac{1}{|U|}\mathbf{B}.\{P(x|u)\} \leq \frac{\delta}{|U|} \quad \Longrightarrow \quad \Pr\left(x^*|u^*,\mathbb{Z},\mathbb{W}\right) \leq \left(\frac{1+2\delta}{3}\right) \equiv \gamma$$

Name: $\{P(\mathbf{x}|\mathbf{u})\}$ **is a „δ-good" box.**

(for any setting ***u**** and outcome ***x****)

Proof. – Linear programming

Estimating Bell values conditioned upon the past

Lemma.- (general)

Random variables W_i , $B_i = f_i(W_i)$, B_i - binary

$\overline{B}_i = \mathbb{E}(B_i | W_{i-1}, \ldots, W_1)$ (conditional mean value)

$Z_k = \frac{1}{k}\sum_{i=1}^{k} B_i$ (empirical average) , $\overline{Z}_k = \frac{1}{k}\sum_{i=1}^{k} \overline{B}_i$

$$\Longrightarrow \Pr(|Z_n - \overline{Z}_n| \geq s) \leq 2e^{-n\frac{s^2}{2}}$$

Proof. – Martingales (Azuma ineq.).

Df. For 4-qubit Bell inequality the protocol runned for the device number ,,j'' accepts iff

$$L_j = \frac{1}{n}\sum_{i=1}^{n} B(\mathbf{x}_i^j, \mathbf{u}_i^j) \leq \left(\frac{1}{2} - \varepsilon\right)^4 \frac{\delta}{2}(1-\mu)$$

Remark: Below – **conditional boxes** made out of global one $P(\mathbf{x}_1, \ldots, \mathbf{x}_n | \mathbf{u}_1, \ldots, \mathbf{u}_n)$

$$P_{x_{<l}, u_{<l}}(x_l | u_l) = P_{\substack{\mathbf{x}_1,\ldots,\mathbf{x}_{i-1} \\ \mathbf{u}_1,\ldots,\mathbf{u}_{i-1}}}(\mathbf{x}_i | \mathbf{u}_i)$$

Lemma .- (specific) Suppose the protocol has accepted. Let condition average

$\overline{B}_i^{SV} := \mathbb{E}_{\mathbf{u}_i | \mathbf{u}_1,\ldots,\mathbf{u}_{i-1} \sim \nu} \mathbb{E}_{\mathbf{x}_i \sim P_{\substack{\mathbf{x}_1,\ldots,\mathbf{x}_{i-1} \\ \mathbf{u}_1,\ldots,\mathbf{u}_{i-1}}}(\mathbf{x}_i|\mathbf{u}_i)} B(\mathbf{x}_i, \mathbf{u}_i)$ and $\overline{B}_i^U$ its ,,fair coin'' analog

(ie. with uniform $\mathbb{E}_{\mathbf{u}_i}$). Let set of **,,$\delta$-bad'' conditional boxes be** $I := \left\{ i : \overline{B}_i^U \geq \frac{\delta}{|U|} \right\}$

$\Longrightarrow |I| \leq (1-\mu)n$ or : # of **,,δ-good'' conditional boxes** (ie. $\overline{B}_i^U \leq \frac{\delta}{|U|}$) satisfies $|K| \geq \mu\, n$

with Pr $\geq$ $1 - 2\exp\left(-n\frac{\delta^2(1-\mu)^2(\frac{1}{2}-\varepsilon)^8}{8}\right)$

Proof. Empir. av. close to arytmetic av. $\frac{1}{n}\sum_{i=1}^{n} \overline{B}_i^{SV}$ + single copy lemma translation to $\overline{B}_i^U$

From $\mu\, n$ number of δ -good boxes to suitable min-entropy source

Lemma.- Consider prob. measure P on sequences $x_1, u_1, \ldots, x_n, u_n$.

If there exist subset K , |K|$\geq \mu\, n$ with all $l \in$ K satisfying $P_{x_{<l}, u_{<l}}(x_l | u_l) \leq \gamma$, $0 \leq \gamma < 1$.

$\Longrightarrow$ $P(x_1, \ldots, x_n | u_1, \ldots, u_n) \leq \gamma^{\mu n}$

Proof.- Obvious

Df. Min-entropy $H_{min}(S) = \min_{s \in supp(S)} \log \frac{1}{\Pr(S = s)}$

Lemma.- Under previous assumption satisfied for all sequences $x_1, u_1, \ldots, x_n, u_n$.

belonging to the set S of meausre $Q > 1 - \delta'$ one has bound for min entropy

$H_{min}(P_{(u_1, \ldots, u_n)}) \geq -\log\left(\frac{\gamma^{\mu n}}{1 - \delta'} + \sqrt{\delta'}\right)$ with Pr $\geq$ $1 - 4\sqrt{\delta'}$ where $P_{(u_1, \ldots, u_n)}$

stands for the distribution $P(x_1, \ldots, x_n | u_1, \ldots, u_n)$.

Proof. – Considering distance to normalised distribution P'=P/Q on S (zero outside S) .

Proposition.- If the test on (possibly correlated in time) single 4-qubit source accepts then with Pr $\geq$ 1- O(exp[-n(½- ϵ)^8 (1-μ)$^2\delta^2$/4))
one gets the source with linear min-entropy

$H_{min} \geq -\log \gamma'^{\,\mu n}$ ($0 \leq \gamma' < 1$).

Proof. - Observe that passing the test leads to $\mu\, n$ number of δ -good boxes which quarantees γ= (1+ 2 δ)/3 and error δ' = 2 exp[-n(½- ϵ)^8 (1-μ)$^2\delta^2$/8)
which is exponential in n (!).

Quantum Mechanics allows to accept the test with hight probability

Question.- *Is it possible that quantum mechanics guarantees the finite Pr(acceptance) ?*

Answer: YES

Proposition.-
Suppose that we apply the above protocol to the box $P(\mathbf{x}_1, \ldots, \mathbf{x}_k | \mathbf{u}_1, \ldots, \mathbf{u}_k)$ such that it satisfies $B.\{P_{x_{<i}, u_{<i}}(x_i|u_i)\} \leq \delta''$ for any i . Then the protocol

with probability *Pr(acceptance)* $\geq 1-$ $\exp[-n(\frac{1}{2}-\epsilon)^8 (1-\mu)^2\delta^2/8)$.

as long as

$$\delta'' \leq \frac{(1-\mu)\delta(\frac{1}{2}-\varepsilon)^4}{4(\frac{1}{2}+\varepsilon)^4}; \quad \approx \quad O(\delta(1-\mu)(1-2\varepsilon)^4).$$

Quantum realisation:
(approximate) quantum iid. source with k slightly mixed 4-qubit states of the form $(1-16\delta'')|\Psi\rangle\langle\Psi| + \delta'' I^{\otimes 4}/16$.

More then one (physical) source of 4-qubit entanglement:
getting two or more linear min-entropy (statistical) sources
via Bell inequality violation

De Finetti –type theorem

Lemma 6. *Let $P(x^1_{\leq n_1}, \ldots, x^k_{\leq n_k} | u^1_{\leq n_1}, \ldots, u^k_{\leq n_k})$ be a time-ordered non-signaling distribution, with output and input alphabets Σ and Λ, respectively (i.e. $P : \Sigma^{\times n} \times \Lambda^{\times n} \to \mathbb{R}^+$). The distribution P represents k devices each with n_j boxes. Let $(a_1, \ldots, a_k) \in [n_1] \times \ldots \times [n_k]$ and $(u^1_{\leq n_1}, \ldots, u^k_{\leq n_k})$ be chosen from an ε-SV source $\nu(a_1, \ldots, a_k, u^1_{\leq n_1}, \ldots, u^k_{\leq n_k})$.*

Then for every set of positive reals $\{t_2, \ldots, t_k\}$,

$$\Pr_{(a_1,\ldots,a_k)\sim\nu} \left(T \geq \sum_{i=2}^{k} \sqrt{\frac{8 \ln(2) t_i^2 \sum_{j=1}^{i-1} n_j}{n_i^{1-\log(1+2\varepsilon)}}} \right) \leq \sum_{i=2}^{k} \frac{1}{t_i}, \tag{33}$$

with

$$T := \mathbb{E}_{u^1_{\leq n_1}, \ldots, u^k_{\leq n_k} \sim \nu_{a_1,\ldots,a_k}} \quad \mathbb{E}_{x^1_{<a_1}, \ldots x^k_{<a_k} \sim P} \left\| q(x^1_{a_1}, \ldots, x^k_{a_k} | u^1_{a_1}, \ldots, u^k_{a_k}) - q(x^1_{a_1} | u^1_{a_1}) \otimes \ldots \otimes q(x^k_{a_k} | u^k_{a_k}) \right\|_1 \tag{34}$$

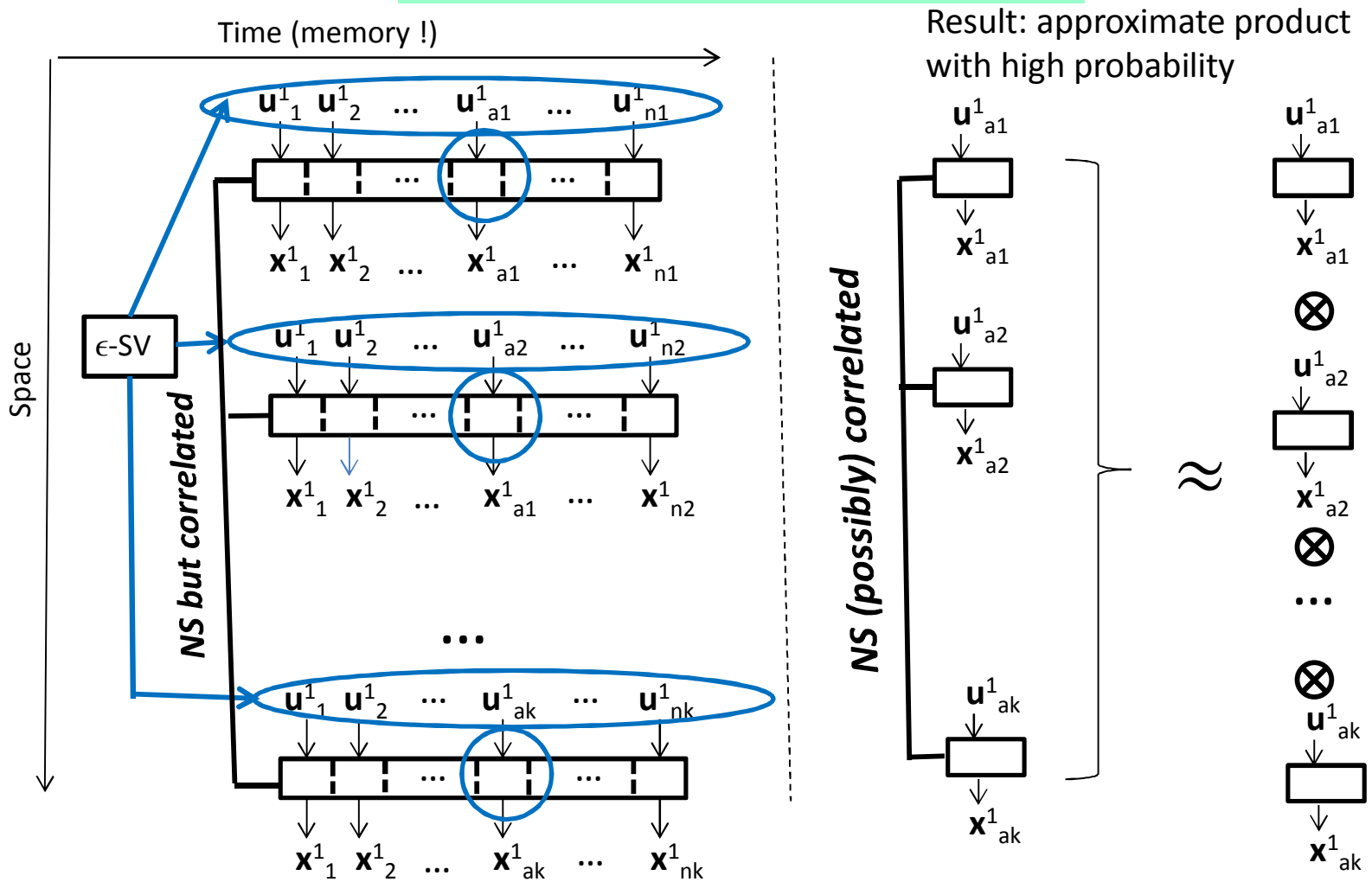
where q is the conditional box given the inputs $u^j_{<a_j}$ and outputs $x^j_{<a_j}$ for all $1 \leq j \leq k$

$$q(x^1_{a_1}, \ldots, x^k_{a_k} | u^1_{a_1}, \ldots, u^k_{a_k}) := P_{\substack{x^1_{<a_1}, \ldots, x^k_{<a_k} \\ u^1_{<a_1}, \ldots, u^k_{<a_k}}} (x^1_{a_1}, \ldots, x^k_{a_k} | u^1_{a_1}, \ldots, u^k_{a_k}), \tag{35}$$

and $\nu_{a_1,\ldots,a_k}$ is the probability ν conditioned on measuring $(a_1, \ldots, a_k)$.

Proof.- Involves application of chain inequality + Pinsker inequality (relating mutual info. to trace norm distance)

De Finetti – type theorem - conclusion



Conclusion.- If $n_1 = 1, \quad n_i^{1-\log(1+2\varepsilon)} = 8\ln(2)k^2t^3 n_{i-1}$ then

$$\Pr\left\{ \left\| q(\mathbf{x}^1_{a_1},\ldots,\mathbf{x}^k_{a_k}|\mathbf{u}^1_{a_1},\ldots,\mathbf{u}^k_{a_k}) - q(\mathbf{x}^1_{a_1}|\mathbf{u}^1_{a_1}) \otimes \ldots \otimes q(\mathbf{x}^k_{a_k}|\mathbf{u}^k_{a_k}) \right\|_1 \leq O(1/\sqrt{t}) \right\} \geq 1 - O(1/\sqrt{t})$$

where $q(x^1_{a_1},\ldots,x^k_{a_k}|u^1_{a_1},\ldots,u^k_{a_k}) := P_{\substack{x^1_{<a_1},\ldots,x^k_{<a_k} \\ u^1_{<a_1},\ldots,u^k_{<a_k}}}(x^1_{a_1},\ldots,x^k_{a_k}|u^1_{a_1},\ldots,u^k_{a_k})$.

De Finetti theorem – extension to blocks

Lemma 17. *Let $P(X^1_{\leq N_1},\ldots,X^k_{\leq N_k}|U^1_{\leq N_1},\ldots,U^k_{\leq N_k})$ be a $(k;N_1n,N_2n,\ldots,N_kn)$ time-ordered non-signaling distribution, with output and input alphabets Σ and Λ, respectively (i.e. $P:\Sigma^{\times(\sum_{i=1}^k N_in)}\times\Lambda^{\times(\sum_{i=1}^k N_in)}\to\mathbb{R}^+$). The distribution P represents k devices with the j-th device containing nN_j boxes. Assume $(A_1,\ldots,A_k)\in[N_1]\times\ldots\times[N_k]$ are chosen using an ε-SV source ν that is uncorrelated with the box P. Then for any probability distribution $\nu(U^1_{\leq N_1},\ldots,U^k_{\leq N_k})$ and for every set of positive reals $\{t_2,\ldots,t_k\}$, we have*

$$\Pr_{(A_1,\ldots,A_k)\sim\nu}\left(T\geq\sum_{i=2}^k\sqrt{\frac{2\log|\Sigma|\ln(2)nt_i^2\sum_{j=1}^{i-1}N_j}{N_i^{1-\log(1+2\varepsilon)}}}\right)\leq\sum_{i=2}^k\frac{1}{t_i},\tag{67}$$

with

$$\begin{aligned}T:=\;&\mathbb{E}_{U^1_{\leq N_1},\ldots,U^k_{\leq N_k}\sim\nu_{A_1,\ldots,A_k}}\mathbb{E}_{X^1_{<A_1},\ldots X^k_{<A_k}\sim P}\\&\left\|q(X^1_{A_1},\ldots,X^k_{A_k}|U^1_{A_1},\ldots,U^k_{A_k})-q(X^1_{A_1}|U^1_{A_1})\otimes\ldots\otimes q(X^k_{A_k}|U^k_{A_k})\right\|_1\end{aligned}\tag{68}$$

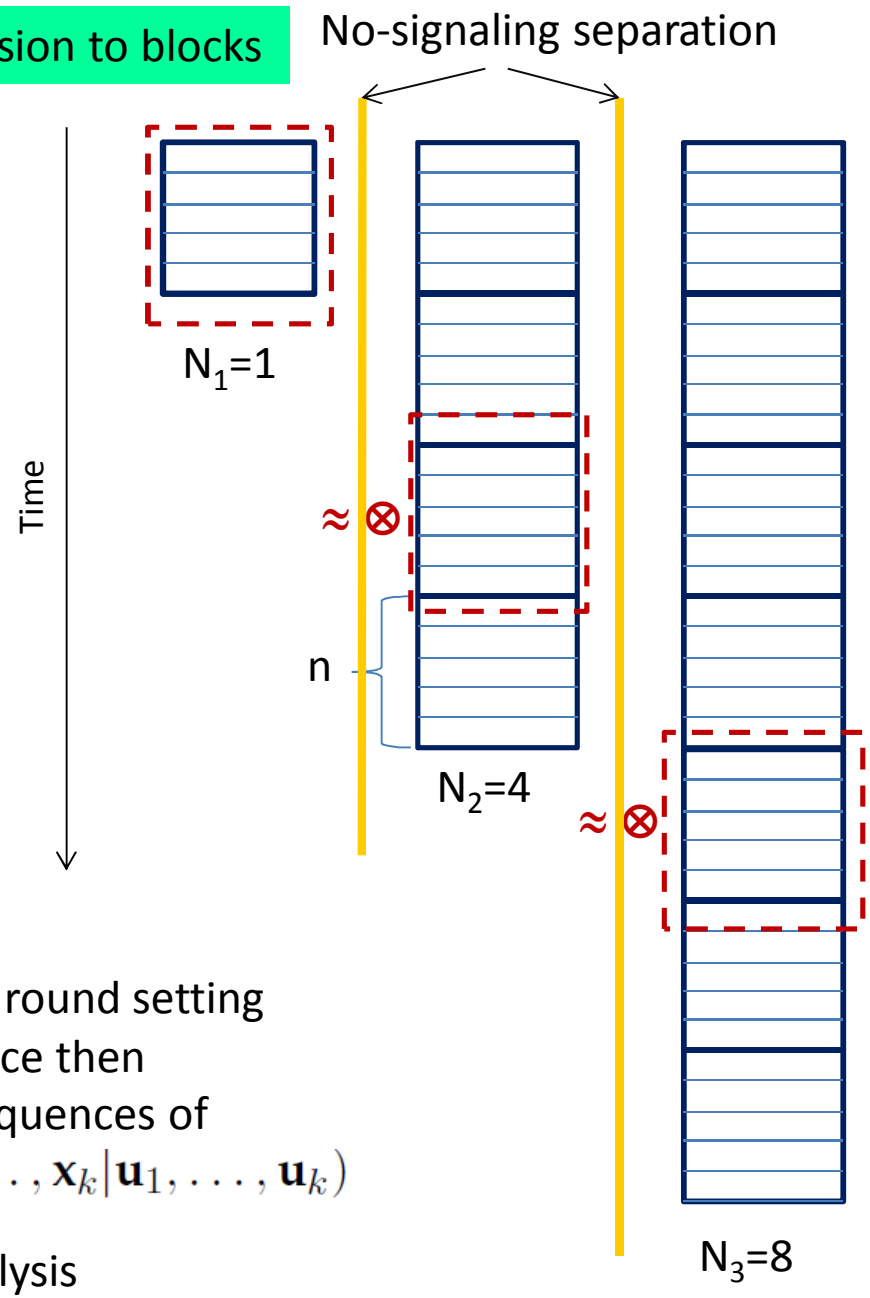
where q is the conditional box given the inputs $U^j_{<A_j}$ and outputs $X^j_{<A_j}$ of all prior boxes for all $1\leq j\leq k$

$$q(X^1_{A_1},\ldots,X^k_{A_k}|U^1_{A_1},\ldots,U^k_{A_k}):=P_{\substack{X^1_{<A_1},\ldots,X^k_{<A_k}\\U^1_{<A_1},\ldots,U^k_{<A_k}}}(X^1_{A_1},\ldots,X^k_{A_k}|U^1_{A_1},\ldots,U^k_{A_k}),\tag{69}$$

and $\nu_{A_1,\ldots,A_k}$ is the probability ν conditioned on measuring $(A_1,\ldots,A_k)$. Moreover, there exist suitable choice of block sizes N_j and reals $\{t_i\}$ such that

$$\Pr_{(A_1,\ldots,A_k)\sim\nu}\left(T\geq\frac{1}{t'}\right)\leq\frac{1}{t'}\tag{70}$$

for some suitably large parameter t'.



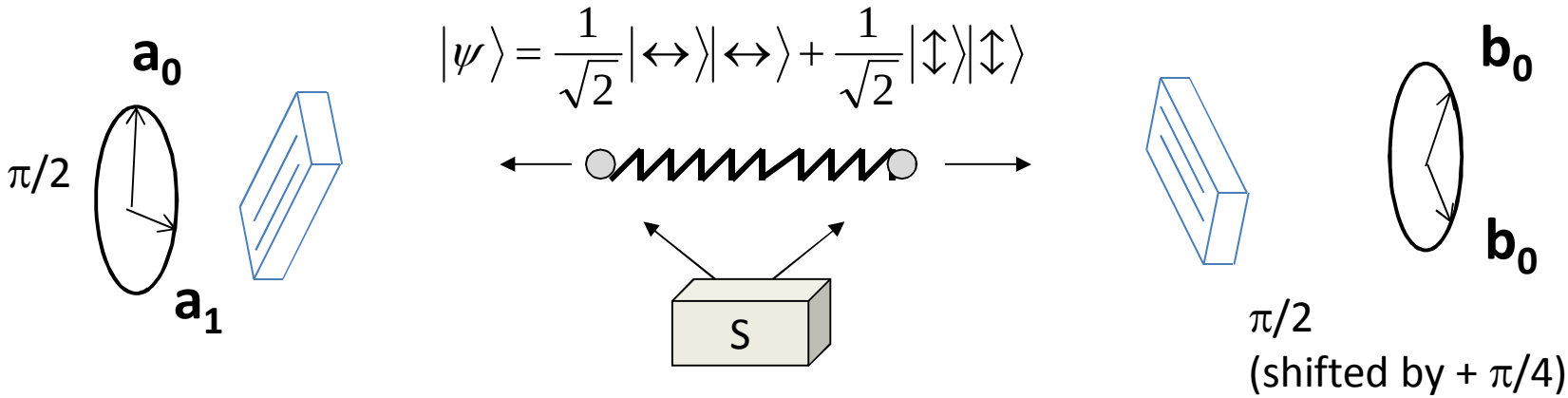
3 quantum sources

Conclusion .-If each n-round block and each single round setting picked up with probability generated by ϵ-SV source then the **blocks** represent products probabilities for sequences of settings with measure $\geq$ 1- O($\sqrt{t}$). Each $P(\mathbf{x}_1,\ldots,\mathbf{x}_k|\mathbf{u}_1,\ldots,\mathbf{u}_k)$

Observation: We are back in the single source analysis
$\Longrightarrow$ each **block** provides linear (statistical) H_{min} source.

Randomness extraction from two or more independent linear (statistical) H_{min} sources

Saturation of Tsirelson bound by maximally entangled state of the two qubits



Lemma 5. *[Extractors Constructions]*

(i) *[2] There exists a (non-explicit) deterministic extractor that given two independent sources of min-entropy larger than h, outputs $\Omega(h)$ bits $2^{-\Omega(h)}$-close to uniform.*

(ii) *[18] There exists an explicit extractor that given three independent sources, one having min-entropy larger than τn (for any $\tau > 0$) and the other two larger than $h \geq \text{polylog}(n)$, outputs $\Omega(h)$ bits $2^{-h^{\Omega(1)}}$-close to uniform.*

[2] B. Chor and O. Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. SIAM Journal on Computing, 17(2): 230 (1988).

[18] A. Rao. Extractors for a constant number of polynomially small min-entropy independent sources. Proceedings of the 38th Annual ACM Symposium on Theory of Computing (2006).

$$N_1 = 1, \quad N_2^{1-\log(1+2\varepsilon)} = 8n\ln(2)t^4$$

$$d_c(S|\mathbb{Z},\mathbb{W}) := \sum_{s=0}^{|\Sigma|-1} \max_w \sum_z P(\mathbb{Z}=z|\mathbb{W}=w)|P(S=s|\mathbb{Z}=z,\mathbb{W}=w) - 1/|\Sigma||$$

$$d_c(S_n|\mathbb{Z},\mathbb{W}) \leq 4\exp\left(-\Omega\left(n\delta^2(1-\mu)^2(\frac{1}{2}-\varepsilon)^8\right)\right)$$

$\Omega(n)$ $\quad S_n$

$$d_c(S|\mathbb{Z},\mathbb{W}) \leq |\Sigma| d(S|\mathbb{Z},\mathbb{W})$$

$O(\delta(1-\mu)(1-2\varepsilon)^4)$-

$S \in \Sigma$

$O(\delta(1-\mu)(1-2\varepsilon)^4)$-

$$d(S|\mathbb{Z},\mathbb{W}) := \max_{s,w,z} |P(S=s|\mathbb{Z}=z,\mathbb{W}=w) - 1/|\Sigma||.$$